LINKSYS®

思科系统公司子公司



宽带防火墙路由器



内建4端口交换机和VPN终点

用户手册



型号 **BEFSX41-CN**

目录

图片清单：

第一章：介绍

欢迎

感谢您选用这款宽带防火墙路由器，它带有 4 端口交换机和 VPN 终点。这款路由器给您的网络提供一种高安全性的方式去共享高速的互联网连接和资源包括文件和打印机。

这是怎么实现的呢? 在这款路由器里，您拥有一台标准的 Linksys 路由器的互联网访问和共享能力，还有 4 端口 10/100 交换机的网络扩展能力和 VPN 的网络安全功能。

但所有这些意味着什么?

在路由器的核心，是一个标准的 Linksys 路由器，它可以在您的网络里，给您提供共享宽带和互联网访问的能力。这也带来了防火墙的保护和您所期望的一台 Linksys 路由器简便的安装与配置。加上了 4 端口 10/100 交换机的网络扩展性。在路由器背面板的 4 个端口都是自动检测的，意味着路由器可以自动分辨您是通过直通线和交叉线连接的，使得它比以往更易使用。最后添加了 VPN 网络安全到路由器，允许您保护数据安全。虚拟专用网络 VPN，创建虚拟隧道，穿过互联网把您的 PC 机和另一台连接起来，在从一端传递到另一端的时候保持数据安全。

在这本用户手册里，您可以找到所有需要用来设置，配置和使用路由器的资料，包括描述 VPN 的附录。欢迎到安全宽带网络来。

内容简介

这本用户手册覆盖了所有您需要了解关于这台路由器的任何资料。另外，除了在章节里给出的如何安装使用它的向导，还有几个附录提供了更多的信息。

- **第一章：介绍**

  这章介绍路由器的应用和这本用户手册

- **第二章：网络基础**

  这章简要解释网络如何工作

- **第三章：了解路由器**

  这章让您快速了解路由器前面板上的指示灯和后面板上的端口

- **第四章：连接到路由器**

  这章指导您如何连接 DSL 调制解调器和 PC 到路由器上

- **第五章：使用路由器基于网页工具**

  这章描述基于网页工具和可用功能，这样您就可以使用它，改变高级配置的设置

- **附录 A：常见故障及处理**

  这个附录介绍一些在安装和使用路由器的过程中可能存在问题和解决方法，还有经常询问的问题。

- **附录 B：升级固件**

  这个附录解释您应该如何升级路由器的固件

- **附录 C：为您的以太网卡查找 MAC 地址和 IP 地址**

  这个附录指导您如何为您的 PC 的以太网卡查找 MAC 地址和以太网地址

- **附录 D：Windows 帮助**

  这个附录告诉您如何使用 Windows 关于网络操作方面的帮助，比如安装 TCP/IP 协议

- **附录 E：最优化 VPN 安全**

  这个附录告诉您如何通过 VPN 隧道发挥 VPN 路由器的最大功效

- **附录 F：在 Windows2000 或者 XP 计算机和 VPN 路由器之间配置 IPSec**

  所以，如何为您的 PC 设置 VPN 隧道? 这个附录会告诉您

- **附录 G：SNMP 功能**

  这个附录告诉您简单网络管理协议

- **附录 H：术语**

  这个附录给出一个网络中常用词语简短的术语表

- **附录 I：规格**

  这个附录提供路由器的技术规范

- **附录 J：保修信息**

  这个附录提供路由器的保修资料

- **附录 K：联系信息**

  这个附录给出各种 Linksys 资源的联系资料，包括技术支持

第二章：您的虚拟专用网络（VPN）

为什么我需要一个 VPN?

计算机网络提供了一种灵活性，这是仅使用纸张所做不到的。然而，正是这个灵活性，也增加了安全方面的风险。这是为什么首先要介绍防火墙。防火墙有助于保护在一个局域网内部的数据。但是，一旦信息发送到您的局域网外，当电子邮件发送到它们的目的地，或者当您在外部网络上不得不连接到您公司的局域网时，您应该怎么办？您的数据如何保护？

那就是 VPN 有用的时候了。VPN 称为虚拟专用网络，因为它们保护数据移动到您的网络外部的时候就像它仍然在那个网络内部一样。

当数据从您的计算机穿过互联网发送到外部的时候，它总是暴露在黑客前面。您也许已经拥有一个防火墙，它会帮您保护周围移动的数据，或者防止在您的网络里的数据被破坏，或者被您的网络外的组织截获，但是一旦数据移到您的网络外部，当您通过电子邮件发送数据给某人或者与互联网上的一个人进行通信的时候，防火墙将不再保护您的数据。

在这时，您的数据将暴露在那些黑客面前，他们用各种手段，窃取您的数据，用户和密码，而且您的网络登录和安全数据。其中一些常用的方法如下：

1） MAC 地址欺骗

无论是在您的局域网或者互联网上，在互联网上传输的数据包是以一个头部先行的。这个数据包的头部包含了数据包有效传输所需要的源和目的地址信息。黑客可以利用这些信息欺骗（或者伪造）网络上允许 MAC 地址。通过这些欺骗的 MAC 地址信息，黑客也可以截取给其他用户的信息。

2） 数据探测

数据“探测”是黑客获取流经不安全网络，比如互联网的数据的一种手段。专门用于这种活动的工具，比如协议分析器和网络诊断工具，常常加入到操作系统中允许以纯文本的方式浏览数据。

3） 中间人攻击

一旦黑客已经探测或者欺骗得到足够的信息，他就可以执行中间人攻击了。这种攻击在数据从一个网络传输到另一个网络的时候执行，把数据重新路由到新的目的地。甚至数据不是为它的目的接收者所接收，它看起来就像这个人正在发送数据过来一样。

这些仅仅是黑客使用的一些手段，他们总是在发展更多的手段。没有您的 VPN 的安全性，您的数据穿越互联网的时候经常暴露在这些攻击的面前。穿越互联网的数据在到达它的最终目的地之前经常绕着世界经过许多不同的服务器。对于非安全的数据而言那是一段很长的路途，这也正是 VPN 服务器的目的所在。

什么是虚拟专用网络?

虚拟专用网络 VPN 是在两个不同网络的两个终端，例如客户机和 VPN 路由器之间进行连接，它允许私有数据通过一个共享的或者公用的网络例如互联网安全地发送。这样建立一个可以在两个局域网或者网络之间安全发送数据的专用网络。

这是通过建立一条“隧道”实现的。一个 VPN 隧道连接两台 PC 或者网络，允许数据传输经过互联网就好像仍然在本地网络内一样。不是直接的隧道，它是一个安全的连接，通过加密数据在两个网络之间发送。

VPN 对于用一条私有的，专用的，租用的线路于专用网络而言是经济划算的。使用工业标准化的加密和认证技术 IPSec（IP 安全的缩写，IP Security）VPN 创建了一条安全的连接，实际上，它操作起来仿佛您是直接连接到您的本地网络一样。虚拟专用网络可以用于创建一个安全的网络用于连接中心办公室和各部门办公室，远程通信者，和/或者外部网络的专业人员（旅行在外的人可以使用任何安装有支持 IPSec 的 VPN 客户端软件（比如 SSH Sentinel）的计算机连接到 VPN 路由器）

有两种创建 VPN 连接的基本方法：

· VPN 路由器到 VPN 路由器

· 计算机（使用支持 IPSec 的 VPN 客户端软件）到 VPN 路由器

VPN 路由器在两个终端之间创建一个 “隧道” 或者频道，这样在他们之间传输的数据是安全的。安装有支持 IPSec 的 VPN 客户端软件的计算机可以是两个终端之一。内建 IPSec 安全管理器（Windows2000 和 Windows XP）的任何计算机允许 VPN 路由器使用 IPSec 创建一条 VPN 隧道（参考 “附录 F：在 Windows2000 或者 XP 计算机和 VPN 路由器之间配置 IPSec”）。其他版本的微软操作系统要求附加的，安装支持 IPSec 的第三方 VPN 客户端应用软件。

VPN 路由器到 VPN 路由器

如下是一个 VPN 路由器到 VPN 路由器的例子。在家里，一个远程终端工作者使用她的 VPN 路由器保持和互联网连接。她的路由器按照她的办公室的 VPN 设置配置。当她连接到她的办公室路由器，两个路由器创建一个 VPN 隧道，加密和解密数据。当 VPN 应用于互联网，距离不是问题。使用 VPN，远程终端工作者就有一条到中心办公室的安全连接，就像她是直接连接的一样。



重要提示：您必须至少有一台 VPN 路由器在 VPN 隧道的一端。在 VPN 隧道的另一端，您必须有另一台 VPN 路由器或者一台带有支持 IPSec 的 VPN 客户端软件的计算机）

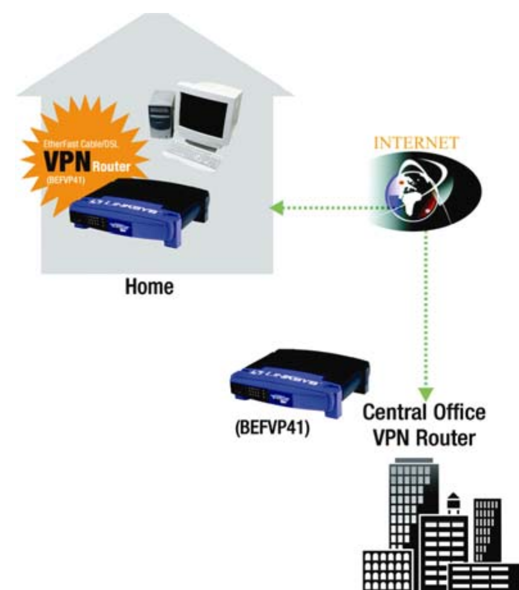


图 2—1：VPN 路由器到 VPN 路由器

计算机（使用支持 IPSec 的 VPN 客户端软件）到 VPN 路由器

下面是一个计算机到 VPN 路由器的例子。在旅馆房间里，一位旅行在外的商人拨通连上他的 ISP。他的笔记本电脑有配置与他的办公室的 VPN 设置一样的 VPN 客户端软件。他访问支持 IPSec 的 VPN 客户端软件，连接到中心办公室的 VPN 路由器。当 VPN 应用于互联网，距离不是问题。使用 VPN，商人就有一条到中心办公室网络的安全连接，就像他是直接连接的一样。

关于创建您的 VPN 的其他资料和步骤请浏览 Linksys 的主页 www.linksys.com 或者参考“附录 F：在 Windows2000 或者 XP 计算机和 VPN 路由器之间配置 IPSec”

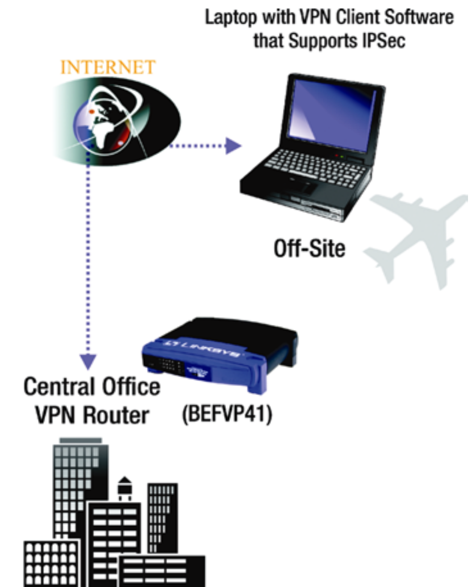


图 2—2 计算机到 VPN 路由器

第三章：了解路由器

后面板

路由器的端口和复位按钮布置在路由器的后面板



图 3－1：后面板

Internet 这个 Internet 端口连接到您的电视电缆或者 DSL 调制解调器上。

1－4 这四个 Ethernet 端口连接到网络设备，比如 PC，打印机服务器或者附加的交换机。

Reset 按钮 这个复位按钮可以有两种使用方式：

如果路由器连接到互联网有问题，用一张纸片或者笔尖按住复位按钮约 1 秒钟。这与按您的 PC 上的复位按钮重新启动机器类似。

如果您遇到与路由器有关极为困难的问题，且已经试过所有其他排除故障的措施，按下复位按钮保持约 30 秒钟。这将恢复路由器的默认设置并且清除所有的路由器设置，比如端口映射或者新密码。

Power Power 端口连接到电源适配器。

前面板

路由器的指示灯布置在前面板，用于告诉您有关的网络活动



图 3－2：前面板

Power 绿色。Power 指示灯在路由器启动的时候点亮。如果指示灯一直在闪烁，则路由器在执行一个诊断测试操作。

Ethernet 绿色。Ethernet 指示灯有两种用途。如果指示灯一直点亮，那么路由器通过相应的端口（1，2，3 或者 4）连接到一个设备上。如果指示灯一直闪烁，则路由器正在那个端口上发送或者接收数据。

Internet 绿色。当路由器连上您的电视电缆或者 DSL 调制解调器上时点亮。

第四章：路由器的连接

概要：

请按照以下步骤设置您的网络：

- 将路由器连接到您的一台电脑。
- 如果有必要，将您的电脑配置为自动从路由器获得 IP 地址。(Windows 98，2000，Me 及 XP 缺省自动获取 IP 地址，因此除非您已经改变缺省设置，否则您无需配置您的电脑)
- 按照您的 ISP 提供的配置来设置路由器。

您互联网服务提供商（下称 ISP）的安装技术人员应该在安装完宽带连接后，将配置信息告诉您。若没有，您可向 ISP 电话询问。当您有了您的互联网宽带连接配置信息，您就可以开始安装并配置路由器了。



图 4－1：一个典型的网络

IP 地址：在网络上用于识别一台计算机或设备的地址。

适配器：一种将网络功能加入您计算机的设备

连接步骤：

1. 在您开始之前，请确认您已经将所有设备的电源关闭，包括路由器，电脑，集线器，交换机及电视电缆或 DSL 调制解调器。
2. 将网络缆线的一端连接到路由器背板上编号端口中的一个。另一端连接到一个网络设备，比如：电脑、打印服务器、集线器或交换机。
   重复此步骤，将电脑及其它网络设备连接到路由器。
3. 将您的电视电缆或 DSL 调制解调器的以太网线连接到路由器的“互联网”端口。
4. 打开电视电缆或 DSL 调制解调器的电源。



重要提示：确认使用 路由器提供的电源适配器。使用不同的电源适配器可能会损坏路由器

5. 连接电源适配器到路由器的“Power”端口。然后将电源适配器连接到电源插座。
   一旦您正确连接了电源适配器，面板上的“Power”指示灯将点亮。
   向后到“第五章：使用路由器基于网页的工具”



图 4－2：连接网络缆线



图 4－3：以太网线连接



图 4－4：连接电源适配器

第五章：使用路由器基于网页的工具

概要

为便于使用，您可以用路由器基于网页工具来管理路由器。本章将解释该工具的所有功能。您可以通过用一根以太网电缆与路由器相连接的电脑使用 Internet Explorer 或 Netscape Navigator 浏览器来访问此工具。

对于基本的网络设置，大多数用户只需要使用工具的以下页面：

- Basic Setup

  在"Basic Setup" 页面中，输入您 ISP 提供的设置。

- Management

  点击"Administration"标签，然后选择"Management"页面。路由器的缺省密码是"admin"。为安全起见，请更改缺省密码。

浏览工具

工具中有六个主要的标签："Setup"、"security"、"Access Restrictions"、"Applications & Games"、"Administration" 及 "Status"。其他的页面在主标签中可用。

Setup（设置）

- Basic Setup – 在这个页面输入互联网连接类型和网络设置。
- DDNS – 启用路由器的动态域名系统(DDNS)功能。
- MAC Address Clone –复制一个 MAC 地址到路由器上。

- Advanced Routing – 在这个页面您可以改变 NAT，动态路由和静态路由的配置。

Security（安全）

- Firewall – 允许您打开或关闭防火墙，阻塞互联网请求，及开启各种的互联网过滤器。
- VPN– 开启虚拟专用网络通过功能，及配置多达 50 个虚拟专用网络隧道。

Access Restrictions（访问约束）

- Internet Access（互联网访问） – 在您的网络中管理互联网访问，阻塞网站。

Applications & Games（应用程序和游戏）

- Port Range Forwarding – 在您的网络中设置公用服务或其他特殊的互联网应用。
- Port Triggering – 为互联网应用程序设置触发范围和转发范围。
- UPnP Forwarding – 改变 UPnP 转发设置。
- DMZ –为了使用特殊的服务允许本地用户暴露于互联网上。

Administration（管理）

- Management – 改变路由器密码，访问权限和 UPnP 设置。
- Log – 在这个页面，您可以浏览或者保存活动日志，甚至发送电子邮件。
- Factory Defaults – 如果您希望恢复路由器默认设置，可以使用这个页面。
- Firmware Upgrade – 在这个页面，您可以升级路由器的固件。

Status（状态）

- Router – 提供路由器及互联网连接的状态信息。
- Local Network – 提供局域网（本地网络）的状态信息。

访问工具页面

为访问路由器基于网页工具，请启动 Internet Explorer 或 Netscape Navigator，并在地址栏中输入路由器的缺省 IP 地址“192.168.1.1”，然后按回车键。



图 5－1：默认 IP 地址

将出现要求您输入用户名和密码的对话框。保留“用户名”栏为空，在“密码”栏填入 admin。然后点击”确定”按钮。



图 5－2：“密码”栏填入 admin

Setup 标签

Setup 标签是您访问路由器基于网页工具时，所见到的第一个页面。此页面分为四个部分：Basic Setup、DDNS、MAC Address Clone 及 Advance Routing。以下将详细描述这些部分。

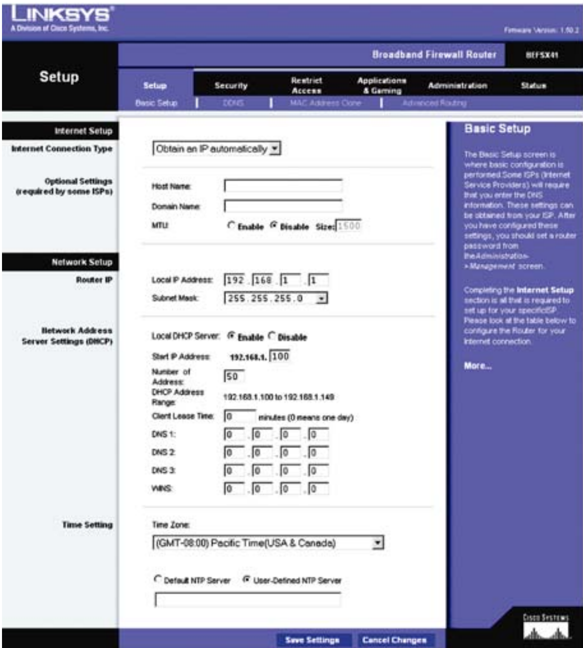


图 5－3：基本配置

Basic Setup（基本配置）

Internet Setup（互联网设置）

此区域允许您选择您网络的互联网使用的配置及连接类型。本路由器支持六种连接类型：“Obtain an IP Automatically (DHCP)”（自动获取 IP 地址）、“Static IP”（静态 IP 地址）、“PPPoE”、

“RAS”、“PPTP”、“L2TP” 及 “Heart Beat Signal”。基本配置页面将会因连接类型不同而变化。

连接类型：Obtain an IP automatically－DHCP（自动获取IP地址）

图 5－4：连接类型: DHCP

缺省情况下，路由器的互联网连接类型被设置为自动获取 IP，这仅在您的 ISP 支持 DHCP 的时候使用。

Host Name (主机名)/ Domain Name(域名)：如果您的 ISP 要求，在此输入主机名和域名。

MTU：此选项制定网络中可传输的最大数据包的大小。如果您想规定这个值，请选择 “Enable”（否则，请保留缺省 “Disable”）输入您所希望的值。该值的取值范围时 1200～1500。大多数 DSL 用户应使用缺省值 1492。

连接类型：Static IP（静态IP地址）

图 5－5：连接类型：Static IP

如果您要使用一个永久 IP 地址，请选择 Static IP（静态 IP 地址）。请从您的 ISP 处获得相关信息。

IP Address 这个 IP 地址是路由器在互联网上所使用的 IP 地址。您的 ISP 将提供给您这个特定的 IP 地址。

Subnet Mask 这是路由器的子网掩码，您的 ISP 将提供给您这个特定的子网掩码。

Default Gateway 您的 ISP 提供给您的默认网关地址。

Primary DNS and Secondary DNS 您的 ISP 将至少提供一个 DNS（域名系统）服务器 IP 地址。

Host Name (主机名)/ Domain Name(域名)：如果您的 ISP 要求，在此输入主机名和域名。

MTU：此选项制定网络中可传输的最大数据包的大小。如果您想规定这个值，请选择 “Enable”（否则，请保留缺省 “Disable”）输入您所希望的值。该值的取值范围时 1200～1500。大多数 DSL

用户应使用缺省值 1492。

连接类型：PPPoE



注意：对于 DSL 用户，如果您需要开启 PPPoE 支持，请记得将您电脑中安装的任何 PPPoE 软件卸载。

一些以DSL技术为基础的ISP使用PPPoE来为终端用户建立互联网连接。如果您使用一根DSL电缆，那先看看您的ISP是否使用PPPoE，如果确实如此，您必须启用这种协议。

User Name andPassword 输入您的ISP提供的用户名和密码。

Service Name 如果您的ISP提供服务名，输入服务名。

Connect on Demand and Max Idle Time 您可以设置您的路由器，让他在一段时间（Max Idle Time）后断开与ISP的连接。如果您已经由于不活动被断开连接，您可以按要求重新让路由器建立连接。如果您想激活它，点击单选按钮。如果您想您的互联网连接一直可用，在*Max Idle Time*栏输入0。否则，输入您希望互联网连接断开前的分钟数。

Keep Alive Option and Redial Period 这个功能会周期性的向ISP发送信号，以保持连接而不断线。缺省的重拨时间为30秒。

***Host Name (主机名)/ Domain Name(域名)*：**如果您的ISP要求，在此输入主机名和域名。

MTU：此选项制定网络中可传输的最大数据包的大小。如果您想规定这个值，请选择 **"Enable"**（否

图 5—6：连接类型：PPPoE

则，请保留缺省 **“Disable”**）输入您所希望的值。该值的取值范围时1200～1500。大多数DSL用户应使用缺省值1492。

修改完成，点击**Save Settings** 按钮。然后点击 *Status*标签，点击**Connect**按钮开始连接。

连接类型：RAS（用于**SingTel**）

远程接入服务Remote Access Service（RAS）是一种仅应用于新加坡的连接服务。新加坡用户请与

SingTel联系，以获取相关信息。

User Name and Password 输入Singtel提供的用户名和密码。

RAS Plan 选择您拥有的计划类型。

Connect on Demand and Max Idle Time 您可以设置您的路由器，让他在一段时间（Max Idle Time）后断开与ISP的连接。如果您已经由于不活动被断开连接，您可以按要求重新让路由器建立连接。如果您想激活它，点击单选按钮。如果您想您的互联网连接一直可用，在*Max Idle Time*栏输入0。否则，输入您希望互联网连接断开前的分钟数。

Keep Alive Option and Redial Period 这个功能会周期性的向ISP发送信号，以保持连接而不断线。缺省的重拨时间为30秒。

Host Name (主机名)/ Domain Name(域名)：如果您的ISP要求，在此输入主机名和域名。

MTU：此选项制定网络中可传输的最大数据包的大小。如果您想规定这个值，请选择 **“Enable”**（否

图 5—7：连接类型：RAS

则，请保留缺省“**Disable**”）输入您所希望的值。该值的取值范围时1200～1500。大多数DSL用户应使用缺省值1492。

修改完成，点击**Save Settings** 按钮。然后点击 *Status*标签，点击**Connect**按钮开始连接。

连接类型：PPTP

点到点隧道协议（Point to Point Tunneling Protocol），是一种仅应用于欧洲和以色列的连接服务。

IP Address 路由器的互联网IP地址，将被互联网用户看到。您的ISP将提供这个地址给您。

Subnet Mask 路由器的互联网子网掩码，将被互联网用户看到，您的ISP将提供这个地址给您。

Default Gateway 您的ISP提供给您的缺省网关地址。

User Name and Password 您在ISP处登陆时使用的用户名和密码。

Connect on Demand and Max Idle Time 您可以设置您的路由器，让他在一段时间（Max Idle Time）后断开与ISP的连接。如果您已经由于不活动被断开连接，您可以按要求重新让路由器建立连接。如果您想激活它，点击单选按钮。如果您想您的互联网连接一直可用，在*Max Idle Time*栏输入0。否则，输入您希望互联网连接断开前的分钟数。

Keep Alive Option and Redial Period 这个功能会周期性的向ISP发送信号，以保持连接而不断线。缺省的重拨时间为30秒。

Host Name (主机名)/ Domain Name(域名)：如果您的ISP要求，在此输入主机名和域名。

图 5－8：连接类型：PPTP

MTU：此选项制定网络中可传输的最大数据包的大小。如果您想规定这个值，请选择 **“Enable”**（否则，请保留缺省 **“Disable”**）输入您所希望的值。该值的取值范围时1200～1500。大多数DSL用户应使用缺省值1492。

修改完成，点击**Save Settings** 按钮。然后点击 *Status*标签，点击**Connect**按钮开始连接。

连接类型：Heart Beat Signal

Heart Beat Signal，是一种仅应用于澳大利亚的连接服务。如果您使用此服务，请与您的ISP联系，以取得必要的配置信息。

User Name and Password 您的ISP提供的用户名和密码。

Heart Beat Server 路由器的互联网IP地址，将被互联网用户看到。您的ISP将提供这个地址给您。

Connect on Demand and Max Idle Time 您可以设置您的路由器，让他在一段时间（Max Idle Time）后断开与ISP的连接。如果您已经由于不活动被断开连接，您可以按要求重新让路由器建立连接。如果您想激活它，点击单选按钮。如果您想您的互联网连接一直可用，在*Max Idle Time*栏输入0。否则，输入您希望互联网连接断开前的分钟数。

Keep Alive Option and Redial Period 这个功能会周期性的向ISP发送信号，以保持连接而不断线。缺省的重拨时间为30秒。

Host Name (主机名)/ Domain Name(域名)：如果您的ISP要求，在此输入主机名和域名。

MTU：此选项制定网络中可传输的最大数据包的大小。如果您想规定这个值，请选择 **“Enable”**（否

图 5－9：连接类型：Heart Beat Signal

则，请保留缺省“**Disable**”）输入您所希望的值。该值的取值范围时1200～1500。大多数DSL用户应使用缺省值1492。

修改完成，点击**Save Settings** 按钮。然后点击 *Status*标签，点击**Connect**按钮开始连接。

连接类型：L2TP

进在您的ISP要求的时候使用L2TP作为连接服务

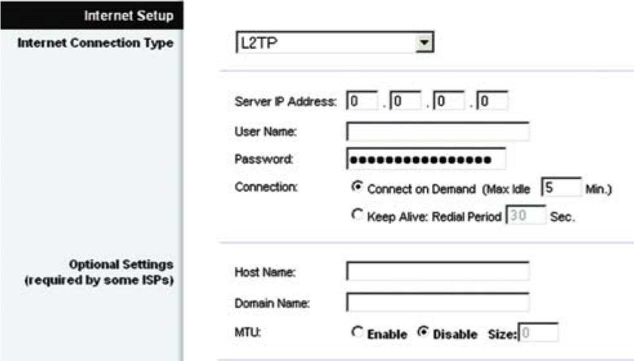


图 5－10：连接类型 L2TP

IP Address 路由器的互联网IP地址，将被互联网用户看到。您的ISP将提供这个地址给您。

User Name and Password 您在ISP处登陆时使用的用户名和密码。

Connect on Demand and Max Idle Time 您可以设置您的路由器，让他在一段时间（Max Idle Time）后断开与ISP的连接。如果您已经由于不活动被断开连接，您可以按要求重新让路由器建立连接。如果您想激活它，点击单选按钮。如果您想您的互联网连接一直可用，在*Max Idle Time*栏输入0。否则，输入您希望互联网连接断开前的分钟数。

Keep Alive Option and Redial Period 这个功能会周期性的向ISP发送信号，以保持连接而不断线。缺省的重拨时间为30秒。

Host Name (主机名)/ Domain Name(域名)：如果您的ISP要求，在此输入主机名和域名。

MTU：此选项制定网络中可传输的最大数据包的大小。如果您想规定这个值，请选择“**Enable**”（否则，请保留缺省“**Disable**”）输入您所希望的值。该值的取值范围时1200～1500。大多数DSL用户应使用缺省值1492。

修改完成，点击**Save Settings** 按钮。然后点击 *Status*标签，点击**Connect**按钮开始连接。

Network Setup（网络设置）

Router IP

路由器的局域网IP地址和子网掩码的值显示在这里，在大多数情况下，保持缺省值。

Local IP Address 缺省值为192.168.1.1。

Subnet Mask 缺省值为255.255.255.0。

Network Address Server Settings (DHCP)

DHCP服务器自动给局域网上的计算机分配IP地址。除非您已有一个，推荐您将路由器设定作为DHCP服务器。

Local DHCP Server 在默认设置中，DHCP已经启用，如果您的网络中已经有一个DHCP服务器，请关闭路由器的这个选项。如果您禁用DHCP，记住为您的路由器设置一个静态IP地址。

Start IP Address 输入DHCP分配的起始IP地址，因为路由器的缺省地址是192.168.1.1，这个值必须是192.168.1.2或更大。

Number of Address（可选）输入您想DHCP服务器分配IP地址数，这个值不能超过253。为了确定DHCP的IP范围，加入开始IP地址（如100）。缺省值为100开始的50个地址，即192.168.1.100至192.168.1.149。

图 5－11：Network Setup

DHCP Address Range 这里显示DHCP地址的范围。

Client Lease Time 客户租借时间是网络用户被容许使用当前的动态IP地址连接路由器的时间总数，输入时间总数，以分钟为单位。输入分钟数，用户便可以“租得”动态IP地址。

Dynamic IP address：DHCP服务器指定的临时IP地址。

Time Setting（时间设置）

为准确运行路由器的日志和其它功能，请在下拉菜单中选择您本地时区。选择**缺省NTP服务器**或者**用户自定NTP服务器**。

修改完成，点击**Save Settings**按钮保存这些改变，或者点击**Cancel Changes**按钮取消您的改变。

DDNS（动态域名系统）

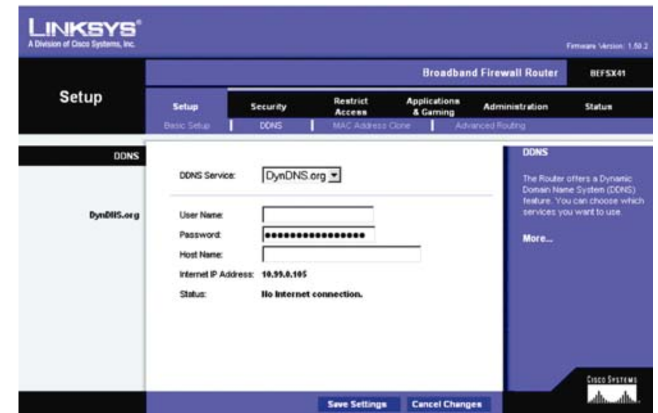


图 5－12：**DDNS**（动态域名系统）

本路由器提供动态域名系统（DDNS）功能。DDNS 允许把一台固定主机或者域名指定给一个动态互联网 IP 地址。如果您正在路由器背后设置自己的网站、FTP 服务器或其它服务器，这将非常有用。

在您使用此功能之前，您需要向两个 DDNS 服务供应商之一， DynDNS.org 或者 TZ0.com 注册 DDNS 服务。如果您不想使用这个功能，请保留缺省值一 “Disable”。

DDNS Service: DDNS服务。如果您的DDNS服务是由DynDNS.org提供的，在下拉菜单中选择“DynDNS.org”。如果您的DDNS服务是由TZ0.com提供的，在下拉菜单中选择“TZ0.com”。在DDNS页面的可用功能会不同，取决于您使用哪一个服务供应商。如果您不想使用这个功能，请保留缺省值一

“Disable” 。

DynDNS.org

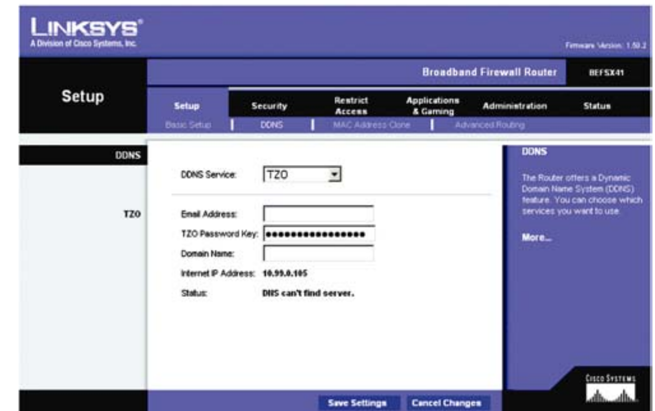


图 5—13：Setup Tab - TZ0.com

User Name, Password and Host Name：输入用户名、密码及您向DynDNS.org提交的帐号的主机名。

Internet IP Address：此处显示路由器的当前IP地址。因为地址为动态，所以此栏会变化。

Status：此处显示DDNS服务连接状态。

TZ0.com Tab

Email Address，TZ0 Password Key, and Domain Name：输入Email地址，TZ0密码和您向TZ0提交的服务的域名。

Internet IP Address：此处显示路由器的当前IP地址。因为地址为动态，所以此栏会变化。

Status：此处显示DDNS服务连接状态。

点击**Save Settings** 按钮保存修改，或者点击**Cancel Changes**按钮取消您的修改。

MAC Address Clone（MAC地址复制）



图 5－14：MAC 地址复制

路由器的MAC地址是一个长度为12位编码，用来标识唯一的硬件。如果您的ISP要求登记您的MAC地址，可参考“**附录C:为您的以太网适配查找MAC地址和IP地址**”来查找您的适配器MAC地址。

MAC Clone Service： 使用MAC地址复制，选择**Enable**。

MAC Address： 在适配器的MAC地址栏中手动填入12位数字地址，然后点击**Save Settings**按钮。

Clone： 如果您想使用您电脑的MAC地址来进行复制，点击**Clone**按钮，路由器将自动探测到您的当前配置电脑的MAC地址，所以您不必告知ISP去改变您的注册MAC地址为路由器的MAC地址。建议使用您向ISP注册的PC机来打开MAC地址复制页面

点击**Save Settings** 按钮保存修改，或者点击**Cancel Changes**按钮取消您的修改 。

Advanced Routing

这一页面容许您配置NAT（网络地址转换），动态路由和静态路由设置。

Dynamic Routing

NAT NAT是一个缺省启用的安全功能。它使路由器能够把局域网的IP地址转变成不同的互联网IP地址。禁用NAT，点击单选按钮**Disable**。（当关闭NAT时，DHCP服务器也将关闭）

使用动态路由可在网络层上自动调节物理变化。路由器使用RIP协议在源和目的数据包之间确定基于最少跳数的网络数据包的路由。RIP协议有规则地向网络上的其他路由器广播路由信息。

Transmit RIP Version 可以挑选以下动态路由协议来传送网络数据：**RIP1**, **RIP1-Compatible**,或**RIP2**。
Receive RIP Version 可以挑选以下动态路由协议来接收网络数据：**RIP1** 或 **RIP2**。

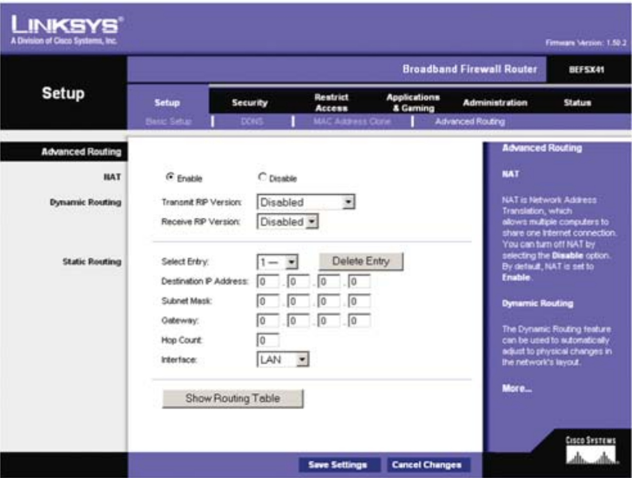


图 5—15：网络地址转换

Static Routing

如果路由器连接到不止一个网络，必须在它们之间设置一个静态路由。静态路由是一条预定路径，网络信息必须沿着这条路径传送到一个指定的主机或者网络。使用静态路由，允许不同的IP域用户通过您的路由器访问互联网。创建一个静态路由，需修改以下设置：

Static Routing（静态路由）：通过固定的隧道转发数据到一个网络

Select Entry 在下拉菜单中选择静态路由号码。本路由器支持多达20个静态路由项。

Delete Entry 如果您想删除一个路由，在下拉菜单选择要删除的静态路由号码，点击**Delete Entry**按钮。

Destination IP Address 目的IP地址时您想要指定静态路由的远程网络或主机的地址。输入您想要创建静态路由的主机IP地址。如果您想建立到整个网络的路由，请确定IP地址的网络部分设为0。例如：路由器的标准IP地址是192.168.1.1。在此基础上，路由网络地址是192.168.1，最后一位数字决定了路由器在网络中的位置。因此，如果您想路由到路由器所在的整个网络，而不是仅仅到路由器，您需要输入192.168.1.0。

Subnet Mask 子网掩码（也称网络掩码）决定了一个IP地址的那个部分是网络部分，哪个部分是网络部分和哪部分是主机部分。例如，一个网络的子网掩码是255.255.255.0。这决定了（使用值255）一个网络IP地址的头三个数字标志这个特定的网络，而最后一位数（从1到254）标志这个确定的主机。

Gateway 这个IP地址应该是用来连接这台路由器和远程网络或者主机的网络设备的IP地址。

Hop Count 数据包将穿梭的网络节点的最大个数。一个节点是网络上的任一个设备，如计算机，打印机，路由器等。

Interface 选择 **LAN** 或 **互联网**，依赖于静态路由的最终目的地。

Show Routing Table 点击**Show Routing Table**按钮来打开现使用的路由表。对于每一个路由，显示目的局域网IP地址，子网掩码，默认网关，跳数和接口，点击**Refresh**按钮更新信息。

点击**Save Settings** 按钮保存修改，或者点击**Cancel Changes**按钮取消您的修改 。

Routing Table Entry List

Refresh

Destination LAN IP	Subnet Mask	Default Gateway	Hop Count	Interface
0.0.0.0	0.0.0.0	10.99.0.2	1	WAN
10.99.0.0	255.255.255.0	0.0.0.0	1	WAN
192.168.1.0	255.255.255.0	0.0.0.0	1	LAN

图5－16：The Routing Table

gateway（网关）：连接不同或不兼容协议网络的设备

Security（安全标签）

安全标签是路由器基于网页工具顶部的第二项。此标签被分为两个页面：Firewall（防火墙）和VPN（虚拟专用网络）。下面将详细介绍：

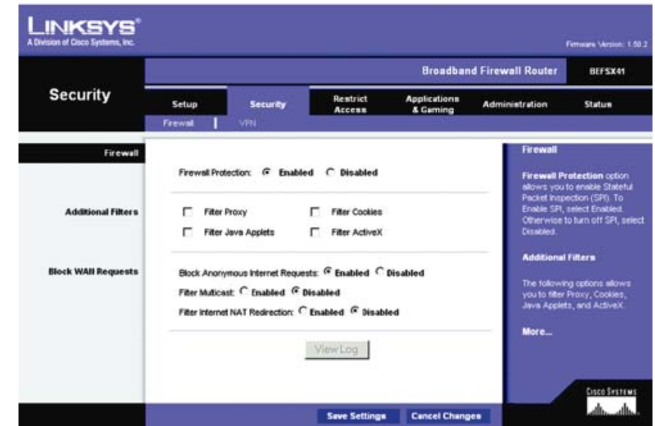


图5－17：安全标签

Firewall（防火墙）

当您点击“Security”时，您首先看到“Firewall”页面。您将可以开启或关闭防火墙。防火墙保护您的网络，还可管理不同的Filter（过滤器），为您提供额外保护。过滤器会阻塞特定的内部用户访问互联网，及阻塞互联网上的匿名请求和多播。

Additional Filters（附加过滤器）

此区域允许您阻塞或过虑特定的互联网应用程序。勾选您想过滤的应用程序前的方框。

- Firewall Protection（防火墙保护）。要添加防火墙保护，点击“**Enabled**”。如果您不需要防火墙保护，点击“**Disable**”。
- Filter Proxy（代理过滤）。使用 WAN 代理服务器可能会损害路由器的安全性。拒绝使用代理过滤将关闭对任何代理服务器的访问。要启动代理过滤，点击“**Enabled**”。
- Filter Cookies（Cookie 过滤）。Cookie 是您与互联网网站交互时，存贮在您的计算机上，并且由网站使用的数据。要启动 cookie 过滤，点击“**Enabled**”。
- Filter Java Applets（Java Applet 过滤）。Java 是网站的编程语言。如果您拒绝 Java Applets，可能导致您不能访问使用这种编程语言创建的互联网网站。要打开 Java Applet 过滤，点击“Enabled”。
- Filter ActiveX（ActiveX 过滤）。Java 是网站的编程语言。如果您拒绝 ActiveX，可能导致您不能访问使用这种编程语言创建的互联网网站。要打开 ActiveX 过滤，点击“**Enabled**”。

Block WAN Request（阻塞广域网请求）

- Block Anonymous Internet Request（阻塞互联网匿名用户请求）。这个通过隐藏您的网络端口防止您的网络被 ping 或者探测，加强您的网络的安全性，因此入侵者用他们的方式攻入您的网络就更困难了。点击 Enable 启动这个功能。

- Filter Multicast（过滤组播）。组播允许多个数据传输同时发送到一个指定的接收者。如果允许组播，那么路由器就允许 IP 组播数据包转发到合适的计算机。选择 Enable 以过滤组播，或者 Disable 以关闭这个功能。

- Filter Internet NAT Redirection(过滤互联网 NAT 重定向)这个功能使用端口映射来防止来自您的局域网的计算机访问本地服务器。

点击**Save Settings** 按钮保存修改，或者点击**Cancel Changes**按钮取消您的修改 。

VPN（虚拟专用网络）

虚拟专用网络（VPN）是一种在两个远程地点之间建立安全连接的安全措施。这里有非常详细的连接配置；以此创建安全性。VPN标签允许您配置VPN设置以使您的网络更加安全。

VPN Passthrough（VPN通过）

IPSec Passthrough（IPSec通过）：互联网协议安全(IPSec) 是在IP层执行数据包安全交换的一套协议。想要允许IPSec通过， 点击Enabled按钮。要禁止IPSec通过， 点击Enabled按钮。

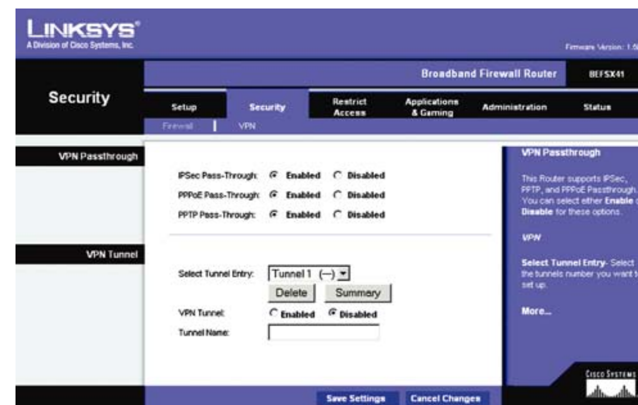


图5－18：虚拟专用网络

PPPoE Pass Through（PPPoE通过） 以太网上点对点协议（PPPoE）允许您的PC机使用您的ISP提供的PPPoE客户端软件。一些ISP可能要求您使用这个功能。想要允许PPPoE通过， 点击**Enabled**按钮。要禁止PPPoE通过， 点击**Enabled**按钮。

PPTP Pass Through（PPTP通过） 点对点隧道协议（PPTP）通过是用来启动VPN到Windows 2000 server会话的方法，想要允许PPTP通过， 点击**Enabled**按钮。要禁止PPTP通过， 点击**Enabled**按钮。

点击**Save Settings** 按钮保存修改，或者点击**Cancel Changes**按钮取消您的修改 。

VPN Tunnel（虚拟专用网络隧道）

建立一个隧道

路由器在两个端点之间创建一个隧道，这样在两点之间的数据或信息是安全的。想要建立这个隧道，在“Select Tunnel Entry”（选择隧道项）下拉菜单中选择您想建立的隧道项。本路由器支持同时创建多达50条隧道。想要删除一个隧道，点击“Delete”（删除）按钮。想要浏览隧道的统计，点击“Summary”（统计）。

然后点击“Enable” 来激活此隧道。

一旦隧道被激活，请在“Tunnel Name”（隧道名字）栏中输入隧道名称。这让您标志多个隧道，不必匹配另一端的名字。

图5－19：虚拟专用网络隧道

Local Secure Group（本地安全组）和Remote Secure Group(远程安全组)

一个本地安全组是指您网络上可以访问此隧道的电脑。远程安全组是指在隧道远程端可以访问此隧道的电脑。在本地安全组和远程安全组页面，您可以选择三个选项之一：子网，IP地址和IP范围。在远程安全组，您还有两个附加选项：主机和任何

Subnet（子网）：如果您选择子网（缺省值），您本地子网中的电脑将可访问此隧道。在使用子网设置时，在IP和子网掩码设置的最后一栏保持为缺省值0。

IP Address（IP地址）：如果您选择IP地址，只有您输入的指定IP地址的电脑才能访问此隧道。

IP Range（IP范围）：如果您选择IP范围，它将是子网子网和IP地址的组合。您可以指定在子网某个IP地址范围的电脑可以访问此隧道。

图5－20：本地安全组和远程安全组

以下选项值用于远程安全组：

Host（主机）：如果您在远程安全组中选择Host（主机）项，远程安全组将与Remote Secure Gateway（远程安全网关）使用相同设置：IP地址，FQDN（正式域名）或者Any（任何）。

Any（任意）：如果您在远程安全组中选择Any（任意）项，本地VPN路由器将接受来自任何IP地址的请求。在隧道远程使用DHCP或PPPoE时，必须使用此项。

Remote Security Gateway（远程安全网关）

远程安全网关是一个在VPN隧道远程端的VPN设备，如另一台VPN路由器。在此区域中有三个选项：IP Address、FQDN及Any。您还可以在此区域中设置加密和认证的方法及级别。

图5－21：远程安全网关

IP Address（IP地址）：选择此项后，请输入连接另一端的VPN设备的IP地址。远程VPN设备可以是另一台VPN路由器、VPN服务器或一台装有支持IPSec的VPN客户端软件的电脑。这个地址可以是静态的（永久的）或者动态的（变化的）——，取决于远程VPN设备的设置。请确认您正确地输入IP地址，否则连接不能够建立。记住，这个不是本地VPN路由器的IP地址而是您想要通信的远

程端VPN；路由器或者设备的IP地址。

FQDN（正式域名）：如果您选择此项，请输入隧道另一端VPN设备的FQDN（正式域名）。远程VPN设备可以是另一台VPN路由器、VPN服务器或一台装有支持IPSec的VPN客户端软件的电脑。FQDN（正式域名）是在互联网上一台指定计算机的主机名字和域名，例如：vpn.myvpnserver.com。

Any（任意）：选择此项后，隧道另一端的VPN设备将接受来自任何IP地址的请求。远程VPN设备可以是另一台VPN路由器、VPN服务器或一台装有支持IPSec的VPN客户端软件的电脑。在隧道远程用户有一个不确定的或者动态IP时（例如在外部网络的专家，或者使用DHCP或者PPPoE的远程通信者），必须使用此项。

Encryption（加密）：使用加密可以使您的连接更加安全。有两种加密方法可供选择：DES和3DES（推荐您使用3DES，以获得更大安全性）。您可以选择任何一个，但您必须保证隧道两端的设备使用相同加密方法。或者您可选择“Disable”，不使用加密。

Authentication（认证）：认证作用于另一个层次的安全。有两种认证方式可供选择：MD5和SHA（推荐使用SHA，以获得更大安全性）。您可以选择任何一个，但您必须保证隧道两端的设备使用相同加密类型。或者您可选择“Disable”，不使用认证。

Key Management（密钥管理）

为使用加密，隧道两端必须就加密和解密方法达成一致。这通过共享一个密钥来实现。在密钥管理中，您可选择自动或手动密钥管理。

Automatic Key Management（自动密钥管理）：选择“Auto (IKE)”，接着在“Pre－shared Key”(预共享密钥)栏中输入一系列的数字和字母。勾选PFS（Perfect Forwarding Secrecy，完全转发保密）旁边的复选框确保初始密钥交换及IKE（互联网密钥交换）是安全的。如例子中所示，使用了**chappy**这个词，如果使用这种方法，隧道两端都必须输入这个词语，基于这个词语，生成一个密钥，用于编码（加密）在隧道上传输的数据和解码（解密）。在这栏您可以使用多达24个数字和字母的

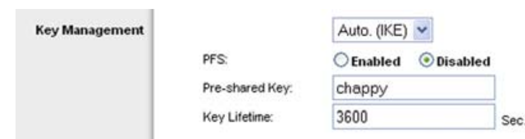


图5－22：密钥管理

组合。不允许有特殊字符和空格，在密钥生命期栏，您可以选择性地让这个密钥在您选择的一段时间后停止使用。输入您想要密钥可用的秒数，或者留空让密钥无限期有效。

Manual Key Management（手动密钥管理）：同样地，您也可以选择手动密钥管理，允许您自行生成密钥。在Encryption Key栏输入您的加密密钥。然后在Authentication Key栏输入您的认证密钥。这两栏必须也和隧道另一端的这两个位置输入的信息相匹配。允许创建多达24个字母的加密密钥，及20个字母的认证密钥。

然而，Inbound SPI（入口SPI）和Outbound SPI（出口SPI）是不同的。这里设置的"Inbound SPI"（入口SPI）的值必须与隧道另一端的Outbound SPI（出口SPI）值相匹配。即，在隧道另一端的Inbound SPI（入口SPI）和Outbound SPI（出口SPI）的值是相反的。在两个栏里只能使用数字。在您点击**Save Settings** 按钮后，十六进制的字符串（一系列的字母和数字）就会显示在Inbound SPI（入口SPI）和Outbound SPI（出口SPI）栏里。

在页面底端的 "Status"（状态）栏在隧道激活时就会显示。

想要连接VPN隧道，点击 **"Connect"（连接）**按钮。若在管理标签的日志页面日志功能启动了，点击 "View Logs" (浏览日志)按钮，就会在一个单独的页面显示您的VPN的活动。需要更多高级VPN选项，请点击 "Advanced Setting" 按钮打开高级设置页面。

点击**Save Settings** 按钮保存修改，或者点击**Cancel Changes**按钮取消您的修改 。

Advanced VPN Tunnel Setup（高级VPN隧道设置）

在高级设置页面，您可以调整特定VPN隧道的设置。

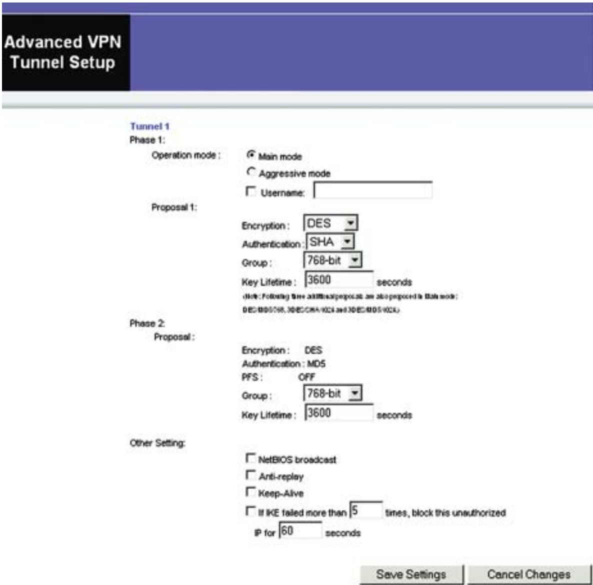


图5－23：高级VPN隧道设置

Phase 1（第一阶段）：第一阶段用于创建一个安全关联（Secure Association，SA），常常称为IKE SA。在第一阶段结束后，第二阶段是用来创建一个或多个IPSec安全关联，用于关键的IPSec会话。

Operation Mode（运行模式）：共有两种模式：Main（主模式）和Aggressive（激进模式）。它们以不同的顺序交换相同的IKE有效载荷。主模式更为常见；然而，一些用户更喜欢激进模式，因为它速度较快。主模式用于普通应用中，比激进模式包含更多的认证要求。推荐您使用主模式因为它更为安全的。不管选择哪种模式，本路由器都会接受远程VPN设备的主模式或激进模式请求。如果隧道一端的用户使用唯一的防火墙标志，这个标志应该输入 “Username” （用户名）栏中。

Encryption（加密）：选择用于加密/解密ESP数据包的密钥长度。可供选择的有两项：DES和3DES。为安全起见，推荐使用3DES。

Authentication（认证）：选择ESP数据包的认证方法。共有两种：MD5和SHA。建议使用更为安全的SHA。

Group（组）：共有两种Diffie-Hellman组可供选择：768位和1024位。Diffie-Hellman是指一种用公共密钥和私有密钥进行加密解密的加密技术。

Key Lifetime（密钥生存期）：在此栏中，您可以选择性地让密钥在您选择的一段时间后失效。输入您想两个终端重新协商生成新的密钥前，当前密钥使用的秒数。

Phase 2（第二阶段）

Group（组）：共有两种Diffie-Hellman组可供选择：768位和1024位。Diffie-Hellman是指一种用公共密钥和私有密钥进行加密解密的加密技术。

Key Lifetime（密钥生存期）：在此栏中，您可以选择性地让密钥在您选择的一段时间后失效。输入您想两个终端重新协商生成新的密钥前，当前密钥使用的秒数。

Other Settings（其它设置）

NetBIOS broadcast（NetBIOS广播）：勾选“NetBIOS broadcast”旁的复选框允许NetBIOS通信通过VPN隧道。

Anti-replay（抗重传）：勾选“Anti-replay” 旁的复选框启动抗重传保护。这个功能跟踪数据包到达的顺序在IP数据包层次上确保安全。

Keep-Alive（保持连接）：勾选“Keep-Alive” 旁的复选框启动保持活动功能，无论何时它掉线了，就会重新建立VPN隧道连接。一旦隧道初始化，这个功能就会保持隧道连接持续一段指定的空闲时间。

Unauthorized IP Blocking（未授权IP阻塞）：勾选“Unauthorized IP Blocking”旁的复选框来阻塞未授权IP地址。在此页面的句子中，说明在您指定的一段时间（秒数）阻塞未授权IP地址多少次后IKE必须失效。

点击**Save Settings** 按钮保存修改，或者点击**Cancel Changes**按钮取消您的修改 。

Access Restrictions（访问约束）

访问约束标签允许您阻塞或允许网络访问，同时管理特定类型的互联网使用。

Internet Access（互联网访问）

互联网 Access Policy（互联网访问策略）：访问通过策略管理。一个策略就是由这个页面的设

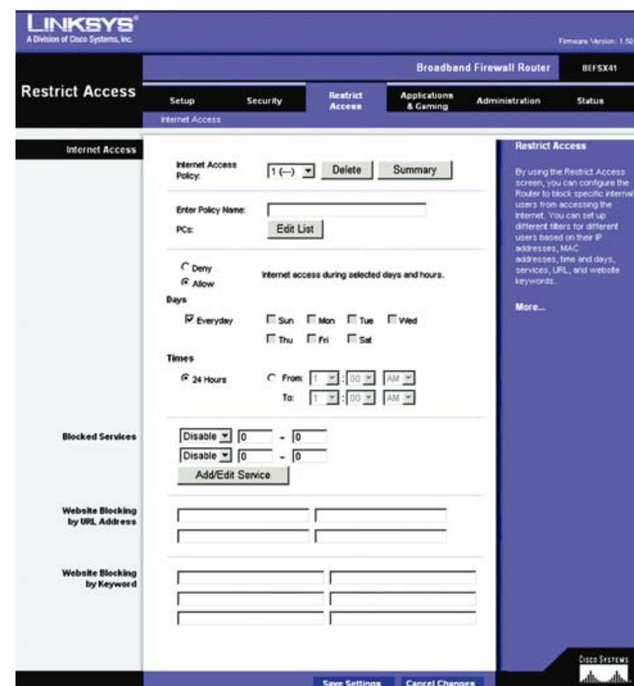


图5－24：访问约束

置建立的（在点击“Save Settings”之后）。从下拉菜单中选择了一个策略，页面上就算会显示这个策略的配置。如果要删除一个策略，选择这个策略的编号，然后点击“Delete”按钮。要查看查看已经建立的策略点击“View Summary”（浏览概要）按钮（策略可以在“View Summary”页面中通过选择一条或者几条策略并点击“Delete”按钮来删除）。

Enter Policy Name（输入策略名）：每一条策略都可以被命名为30个字符以内的名字，以便于记忆。

PCs（电脑）：点击“Edit List”按钮，来选择此策略对哪些计算机有效。您可以输入该计算机的MAC地址或IP地址，如果您想将此策略应用于一组计算机，您可以输入一个IP地址范围。按“Save Settings”保存设定，或按“Cancel Change”放弃改动。

Days/Times（日期/时间）：这条策略什么时候有效？在每一天？在某个时间？在这节里选择您想在某段时间允许或者拒绝访问。选择某一天或者选择 **Everyday**（每一天）。选择这条策略生效的时间，**24 Hours**（24 小时）或者多少小时范围。

Blocked Services（阻塞的服务）：阻塞特定端口服务，例如：POP3、SNMP等。在下拉菜单中选择您想阻塞的服务，在旁边的栏中输入端口范围。如果服务未列出，您可以点击“Add/Edit Service”（添加/编辑服务）按钮来添加或编辑服务。

Website Blocking by URL Address（通过URL阻塞网站）：在这些栏内输入您想要阻塞任何网站的URL。

Website Blocking by Keyword（通过关键字阻塞网站）：如果您不知道您想阻塞的网站的地址，

Internet Policy Summary

No.	Policy Name	Days	Time of Day	Delete
1.	---	S M T W T F S	24 Hours	☐
2.	---	S M T W T F S	24 Hours	☐
3.	---	S M T W T F S	24 Hours	☐
4.	---	S M T W T F S	24 Hours	☐
5.	---	S M T W T F S	24 Hours	☐
6.	---	S M T W T F S	24 Hours	☐
7.	---	S M T W T F S	24 Hours	☐
8.	---	S M T W T F S	24 Hours	☐
9.	---	S M T W T F S	24 Hours	☐
10.	---	S M T W T F S	24 Hours	☐

Close

图5－25：Summary

您可以在此输入网站的关键字。路由器将阻塞到使用这些关键字网站的访问。

创建一个互联网访问策略：

1．在栏中输入策略名。选择 **“Internet Access”** 作为策略类型。点击 **“Edit List”** 按钮。这将打开电脑列表页面，如图 6－25。在此页面中，您可以输入应用此策略任何 PC 机的 IP 或 MAC 地址。您甚至可以输入一个 IP 地址范围。点击 “Apply” 按钮保存设置，“Cancel” 按钮取消改动，及 “Close” 按钮回到 Filter（过滤器）标签。

2．如果您想阻塞或允许那些您列在 PC 列表中 PC 机的互联网访问，点选相应选项。

3．您从 “Blocked Services” 旁边的下拉菜单选择一个服务，用来过滤到互联网上的各种服务的访问，例如 FTP 或者 Telnet。如果一个服务未被列出，您可以点击 “Service” 按钮打开服务页面，如图 6－26 所示，然后添加一个服务到列表。您需要输入 “Service Name”（服务名），同时还有服务使用的 “Protocol”（协议）和 “Port Range”（端口范围）。

4．选择　“Days and Time”（日期和时间）旁边合适的设置，选择过滤互联网访问的时间。

5．最后，点击 “Save Settings”（保存设置）按钮激活这个策略。

图5－26：List of PCs

创建一个入口通信策略

1．在栏中输入策略名。选择 **“Inbound Traffic”** 作为策略类型。

2．输入您想要阻塞的IP地址。选择协议：TCP，UDP或者Both（两者）。输入Port端口号或者选择Any。

3．选择“Deny“（拒绝）或者”Allow“（允许）。

4．选择 “Days and Time”（日期和时间）旁边合适的设置，选择过滤入口通信的时间。

5．最后，点击“Save Settings”（保存设置）按钮激活这个策略。

完成更改后，点击“Save Settings”按钮保存设置，或点击“Cancel Changes”按钮取消更改。

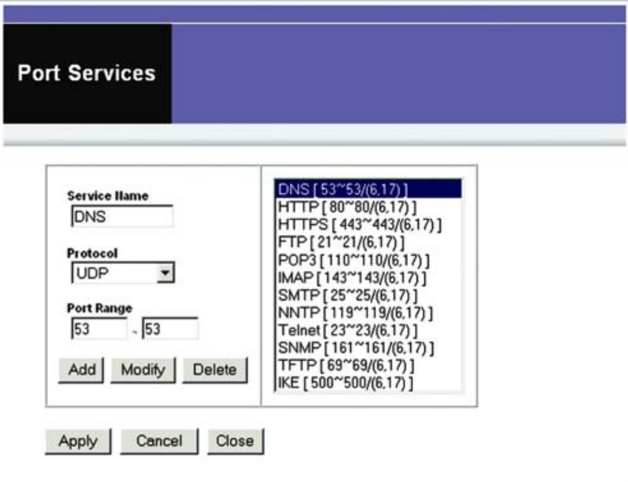


图5－27：保存设置

互联网访问可以通过 URL 地址，在“Website Blocking by URL Address”栏输入网址，在“Website Blocking by Keyword”中的一栏输入一个关键字来过滤。

点击**Save Settings** 按钮保存修改，或者点击**Cancel Changes**按钮取消您的修改 。

Application and Gaming（应用程序及游戏）

Application and Gaming（应用程序及游戏）标签允许您管理用于各种互联网应用程序和游戏的端口。

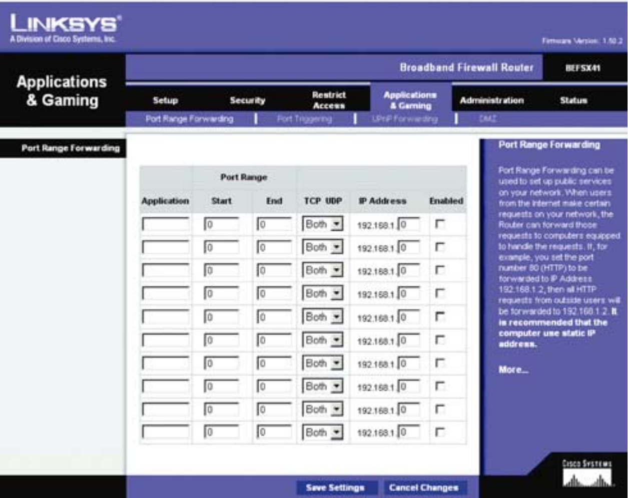


图5－28：应用程序及游戏

Port Range Forward（端口范围转发）

当您点击应用程序及游戏标签时，您会见到“Port Range Forward” （端口范围转发）页面。

端口范围转发在您网络上安装公共服务，比如网页服务器，FTP服务器，Email服务器或其他专用的互联网应用（专用的互联网应用是指用互联网访问来完成特定功能的任何应用程序，如视频会议，或在线游戏。一些互联网应用程序不需要端口转发。）当用户通过互联网向您的网络发送请求，路由器将转发这些请求到适当的电脑。

在使用转发前，请分配一个固定IP地址指定的电脑。

如果您需要将所有端口转发到一台电脑，请点击**DMZ**标签。

要添加使用端口范围转发的服务器，请完成下栏：

Application：在此行中您的应用程序的名称。

Start and End：输入服务器和互联网应用程序使用的外部端口号或者范围。查阅互联网应用程序软件文档获取更多的资料

Protocol：选择协议，TCP 、UDP 或 Both（两者）。

IP Address：输入您想让互联网用户可以访问的服务器的 IP 地址。要查找 PC 机的 IP 地址，转到**附录 C：为您的以太网卡查找 MAC 地址和 IP 地址**

Enable：选择“Enable”复选框启动您定义的服务。如果不勾选“Enable”复选框，端口范围转发功能就不会启动。缺省是关闭（未勾选）。

按“Save Settings”保存设定，或按“Cancel Changes”按钮取消您的修改。

Port Triggering（端口触发）

路由器允许路由器监视指定端口号的外出数据。路由器记住发送匹配数据的计算机的IP地址，这样当请求数据返回通过路由器，通过IP地址和端口映射规则，数据回送到合适的计算机。

Port Triggering（端口触发）

Application 输入触发的应用程序名称。

Triggered Range（触发范围）

对于每一个应用程序，列出触发端口范围。查阅互联网应用程序软件文档关于使用的端口号

Start Port 触发范围的起始端口号。

End Port 触发范围结束端口号。

Forwarded Range（转发范围）

对于每一个应用程序，列出转发端口范围。查阅互联网应用程序软件文档关于使用的端口号

Start Port 转发范围的起始端口号。

End Por 转发范围结束端口号。

点击Save Settings 按钮保存修改，或者点击Cancel Changes按钮取消您的修改。

UPnP Forwarding（UPnP转发）

UPnP Forwarding（UPnP转发）显示预设应用程序设置及给其他应用程序定制端口服务的选项。

UPnP Forwarding（UPnP转发）

Application 这里提供了10个预设应用程序，您可以再添加5个应用程序在剩下的栏里。

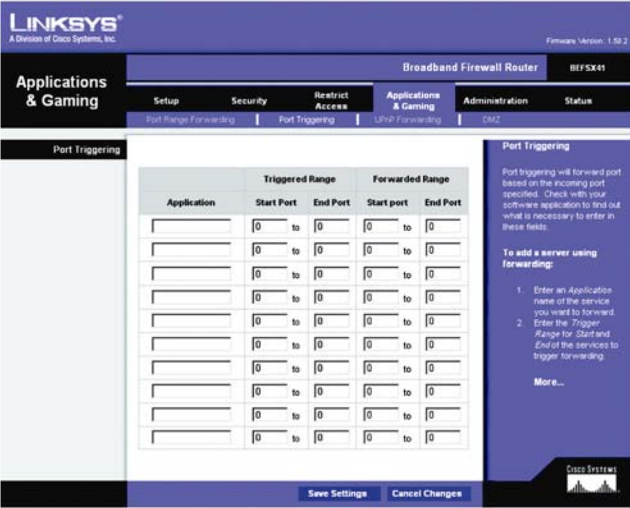


图5－29：端口触发

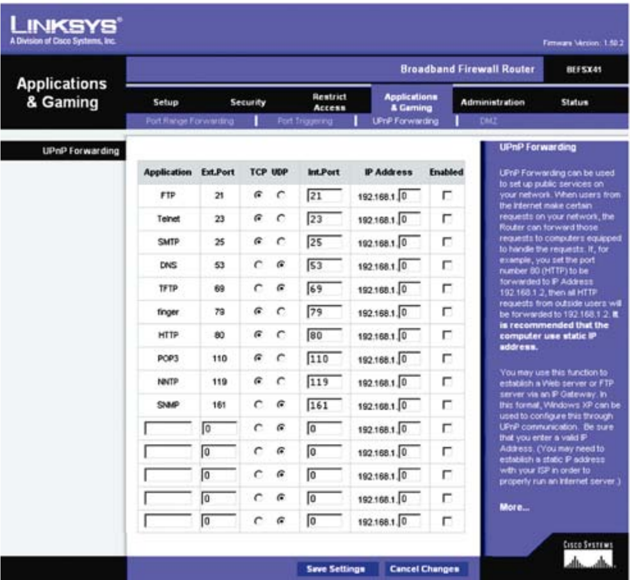


图5－30：UPnP转发

预设的应用程序是最广泛使用的互联网应用程序，他们包括如下的应用程序：

“FTP”（文件传输协议）：一个在TCP/IP 网络(互联网, UNIX等)上用来传输文件的协议。例如在本地机器上为一个网站开发HTML网页后，它们典型地使用FTP上传到网页服务器。

“Telnet”：一种终端模拟协议，常常用于互联网或基于 TCP/IP 的网络。它允许用户在一个终端或计算机上登录到远程设备和运行程序。

“SMTP”（简单邮件传输协议）：这是互联网使用的标准 E-mail 协议。它是一个定义了消息格式和消息传输代理（MTA）的 TCP/IP 协议，用来存储和转发邮件。

“DNS”（域名系统）：将互联网域名定位及翻译成 IP 地址的方法。域名就是一个有意义和便于记忆“处理”的互联网地址。

“TFTP”（简单文件传输协议）：TCP/IP FTP 协议的一个版本，没有目录或密码功能。

“Finger”：一个被广泛用于互联网上的UNIX 命令，用于查找某一特定用户的信息如电话号码，用户当前是否登录和最近一次登录的时间。被“finger”的人必须将他的信息放在系统上以便资料可用。“finger”要求输入完整的user@domain address（用户名@域名地址）。

“HTTP”（超文本传输协议）：用于连接万维网的通讯协议。它的主要功能就是和网页服务器建立一个连接并把 HTML 网页传输到客户端网页浏览器。

“POP3”（邮局协议 3）：互联网上的邮件服务器通常使用的标准。它用于储存收到的 E-mail

直到用户登录并下载。POP3 是一个带很少选择性的简单系统。所有挂起的消息和附件同时被下载。POP3 使用 SMTP 协议。

"NNTP"（网络新闻传输协议）：此协议被用于连接互联网上的 Usenet 新闻组。Usenet 新闻阅读器支持 NNTP 协议。

"SNMP"（简单网络管理协议）：一种广泛应用的网络监视和控制协议，数据从 SNMP 代理（它们是在每个网络设备——集线器，路由器，网桥等，处理报告活动的硬件和/或软件）传送到用于监视网络的工作站控制台，代理返回保存在 MIB（管理信息数据库）中的信息，它们是一种数据结构，定义了设备上什么可取用的和什么可以被控制的（打开，关闭等）。

"Ext. Port"：在此栏中输入服务器所用的外部端口号，查阅互联网应用程序文档获取更多的资料。

"TCP or UDP"：请给每一个应用程序选择协议，UDP 或者 TCP。您也可以两者都选择。

"Int. Port"：在此栏中填入服务器使用的内部端口，查阅互联网应用程序文档获取更多的资料。

IP Address：输入您想让互联网用户可以访问的服务器的 IP 地址。要查找 PC 机的 IP 地址，转到**附录 C：为您的以太网卡查找 MAC 地址和 IP 地址**

Enable：选择"Enable"复选框启动您定义的服务。如果不勾选"Enable"复选框，端口范围转发功能就不会启动。缺省是关闭（未勾选）。

点击Save Settings 按钮保存修改，或者点击Cancel Changes按钮取消您的修改 。

DMZ

在DMZ主机标签，您可以设置Port 4/DMZ到DMZ或者以太网连接。不使用防火墙保护，任何互联网上的用户可以在DMZ主机访问进入与外出数据。这个功能用于特殊目的的服务比如互联网游戏和视频会议。Port 4是专用于DMZ的端口，只有一台计算机可以处于DMZ模式。但是Port Range Forwarding（端口映射）只能转发最多10个端口范围，而DMZ主机可以同时给一台计算机转发所有的端口。

"DMZ Port"（DMZ 端口）要使用这个功能，选择"Enable"，要关闭这个功能，选择"Disable"。

DMZ 主机地址

Assigned by the DMZ Port（通过DMZ端口指定）. DMZ主机是直接或者通过一个集线器或交换机连接到路由器的Port 4/DMZ （端口4/DMZ）的第一台PC机。路由器仅允许一台PC机成为DMZ 主机。

Specify an IP Address behind the DMZ Port（指定DMZ端口后的IP地址）.如果您有多部PC机通过集线器或者交换机连接到Port 4/DMZ （端口4/DMZ）您可以指定哪一部PC是DMZ主机。要公开一台指定IP地址的计算机，在这栏输入那部计算机的IP地址。要查找PC机的IP地址，转到**附录C：为您的以太网卡查找MAC地址和IP地址**

Specify a MAC Address behind the DMZ Port.（指定DMZ端口后的MAC地址）.如果您有多部PC机通过集线器或者交换机连接到Port 4/DMZ （端口4/DMZ）您可以指定哪一部PC是DMZ主机。要公开一台指定MAC地址的计算机，在这栏输入那部计算机的MAC地址。要查找PC机的IP地址，转到**附录C：为您的以太网卡查找MAC地址和IP地址**

Current DMZ Host（当前DMZ主机）.当前DMZ主机的IP地址显示在这里

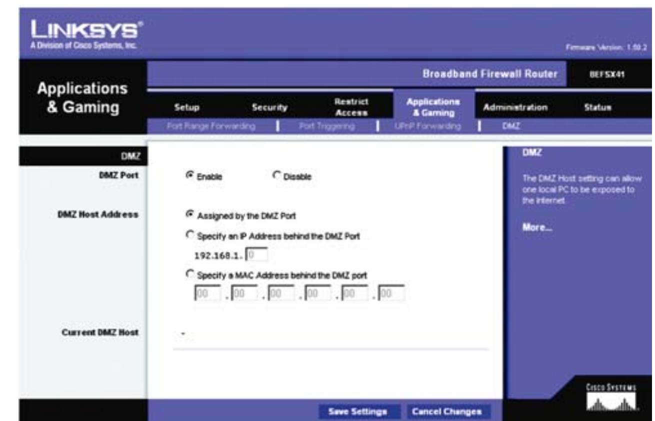


图5－31：应用程序与游戏标签 - DMZ

DMZ (Demilitarized Zone，非军事区)：对一台电脑去除防火墙保护，允许它在互联网上"可见"

点击“Save Settings”按钮保存配置，或点击“Cancel Changes”，取消改变。

Administration（管理）



图5－32：Administration管理标签

Management（管理）

当您点击 Administration 标签，您将见到“Management”页面。这里允许您改变路由器访问配置，及配置 UPnP（通用即插即用）功能。

Router Password（路由器密码）

Local Router Access（本地路由器访问）

为路由器保证安全，当您访问路由器基于网页工具时将要求您输入密码。缺省密码是“admin”。

Router Password（路由器密码）：建议您更改缺省密码。

Re-Enter to confirm（重新输入以确认）：重新输入路由器的新密码，以确认。

Remote Router Access（远程路由器访问）

此功能允许您通过互联网从远程位置访问路由器。

Remote Administration（远程管理）：此功能允许您通过互联网从远程位置管理路由器。点击“Enable”单选框激活远程管理功能。

Administration Port（管理端口）：输入您用于远程访问路由器的端口号。

SNMP（简单网络管理协议）

本路由器支持简单网络管理协议，一种应用广泛的网络监控协议。此功能允许网络管理员通过网络管理系统（如：HP OpenView）监视路由器。

Enable/Disable（开启/关闭）：选择“Enable”开启 SNMP，或选择“Disable”关闭。

Get Community（读取组）：输入允许只读访问路由器 SNMP 信息的密码。

Set Community（设置组）：输入允许读写访问路由器 SNMP 信息的密码。

UpnP

UPnP。UPnP允许WindowsXP给各种互联网应用程序自动配置路由器，例如游戏和视频会议。选择“Enable”激活UPnP特性。因为允许这个功能可能会有安全风险，所以缺省关闭。想让用户修改配置，选择**Enabled**，要允许用户关闭互联网访问，选择**Enabled**。

点击“Save Settings”按钮保存配置，或点击“Cancel Changes”，取消改变。

Log（日志）

“Log”页面提供对互联网连接所有出入URL和IP地址做电子邮件警告和日志的选项。

Email alerts（电子邮件警告）：如果要开启关于类似拒绝服务（Denial of Service）攻击事件的电子邮件警告，请点击“Enable”旁边的单选框。如果不需要启动此功能，请点击“Disable”旁的单选框。

Denial of Service Thresholds（拒绝服务门限）：这个门限就是在路由器发送电子邮件警告前的拒绝服务攻击数量，从20到100。

SMTP Mail Server（简单邮件传输协议邮件服务器）：此处填写邮件服务器的IP地址或域名全称。



图5－33：Administration日志

Email address for alter logs（警告日志的电子邮件地址）：此处填写您想要发送电子邮件警告的邮件地址。

Return email address（回复邮件地址）：可能您的邮件服务器需要您填写邮件回复地址。请在此处输入。如果您不清楚如何填写，请输入与“Email address for alert logs”栏中相同的地址。

Log（日志）：如需要访问日志，勾选Enable单选框。勾选Disable关闭此功能。开启日志后，您可以选择浏览临时日志（点击Incoming Log 按钮或者Outgoing Log 按钮，然后点击View Logs按钮）。您可以选择All（所有日志）, System Log（系统日志）, Access Log（访问日志）, Firewall Log（防火墙日志）和 VPN Log（VPN日志）。点击Clear 按钮清楚所有信息。点击Clear按钮刷新页面。

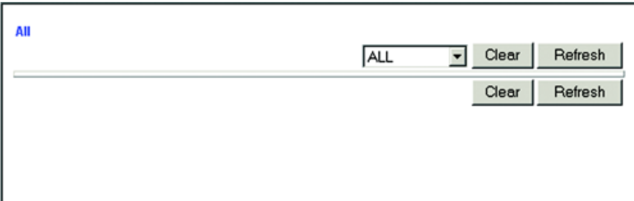


图5－34：View Log

Logviewer IP Address（Logviewer IP地址）：为获得永久的日志记录，必须使用Logviewer软件。此软件可通过Linksys网站www.linksys.com下载。Logviewer会将所有进出活动记录保存到您电脑硬盘上的一个文件中。在Logviewer IP地址栏中输入运行Logviewer软件的电脑的静态IP地址。路由器将更新日志发送到那台电脑。

点击“Save Settings”按钮保存配置，或点击“Cancel Changes”，取消改变。

Diagnostics（诊断）



图5－35：诊断

诊断允许您检查您网络部件的连接状况，还可通过互联网检查您网络外位置的连接。

Ping Target IP（Ping目标地址）：此处填写您希望测试的电脑或网络设备的IP地址，或您网络外的IP地址。

Ping Size（Ping数据包大小）：输入在Ping测试中发送的数据量大小，单位字节。范围是60至1514，

数字越大传送的数据量越大。

No. of Pings（Ping的次数）：输入您想要路由器在这次测试中Ping目的地的次数。范围是1至4。

Ping Interval（Ping间隔）：路由器进行两次Ping之间的时间间隔，单位毫秒。其取值范围在0至9999毫秒之间。

Ping Timeout（Ping超时）：路由器在失败的测试超时前等待的时间。一个失败的测试是指目的地对Ping不作响应。取值范围是0至9999毫秒。

Start Test（开始测试）：点击“Start Test”按钮开始诊断测试。

测试结果将在“Stat Test”按钮下方列出。

按“Save Settings”保存设定，或按“Cancel Changes” 取消改动。

Factory Defaults（默认设置）

Factory Defaults（默认设置）页面允许您恢复路由器的默认设置。



图5－36：恢复出厂设置

Restore Factory Defaults（恢复出厂设置）：选择“Yes”单选按钮清除所有路由器的设置，恢复到默认设置。

点击“Save Settings”按钮恢复到出厂缺省配置，或点击“Cancel Changes”，取消改动。



注意：除非您使用时遇到困难，并已用尽其它故障处理措施，请不要恢复默认设置。一旦路由器复位了，您将不得不重新输入所有设置。

Firmware Upgrade（固件更新）

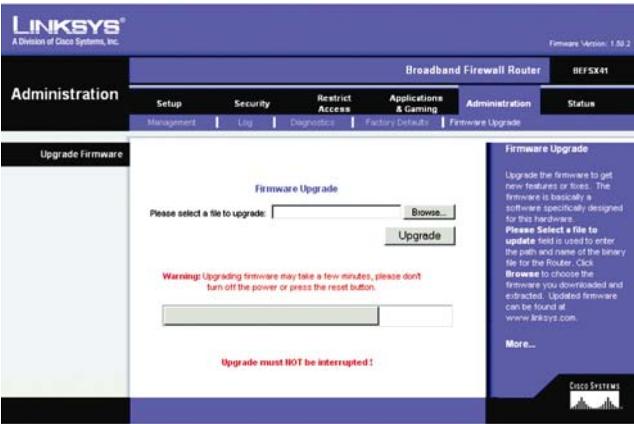


图5－37：固件更新

固件更新页面允许您更新路由器的固件。

在升级之前，请在Linksys网站www.linksys.com下载路由器固件升级文件，然后将其解压缩。

File Path（文件路径）：在此栏中，输入已解压缩的固件升级文件，或点击“Browse”按钮来查找此文件。

Upgrade（升级）：在您选择了合适的文件后，点击“Upgrade”按钮（在此页面的底部），然后按照屏幕显示操作。



注意：如果您升级路由器固件，您可能会丢失现有配置。

Status（状态）

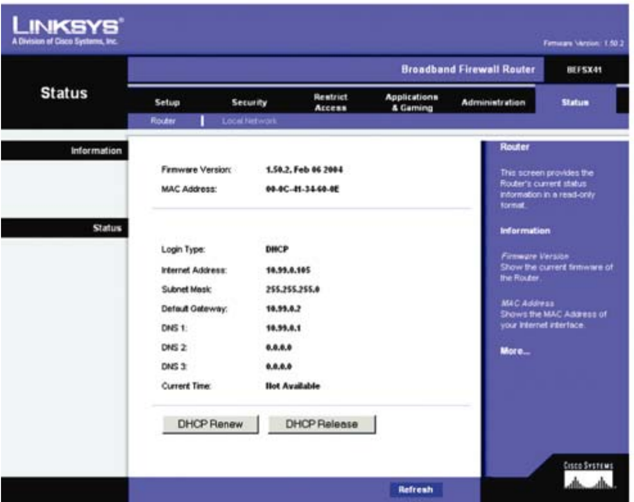


图5－38：登录类型

当您点击“Status”标签，您将会见到“Router”（路由器）页面。此处显示路由器及其设置的信息。

Router（路由器）

Information（资料）

Firmware Version（固件版本）．这里显示路由器的固件版本号

MAC Address（MAC地址）：路由器互联网接口MAC地址在此处显示。

Internet Connection（互联网连接）

Login Type（登录类型）．您的互联网连接类型将在此处显示。

Internet IP Address （互联网IP地址）：您当前的IP地址将会在此显示。

Subnet Mask and Default Gateway子网掩码与默认网关）：这里显示DHCP和静态IP连接的路由器子网掩码及默认网关地址。

DNS 1-3. 这里显示路由器当前使用DNS（动态域名系统）的IP地址

Current Time（当前时间）.如Setup（设置）标签所选的那样，这里显示在您的时区的当前时间



图5－39：路由器状态

DHCP Renew（DHCP更新）. 点击**DHCP Renew按钮**，用新的IP地址替换您的路由器的当前IP地址

DHCP Release（DHCP释放）. 点击**DHCP Release** 按钮删除您的路由器的当前IP地址

点击 **"Refresh"** 按钮，更新当前页面信息。

Local Network（本地网络）

"Local Network" 页面显示本地网络的信息。

DHCP Active IP Table

Refresh

DHCP Server IP Address: 192.168.1.1

Client Hostname	IP Address	MAC Address	Interface	Delete
gjaifzz	192.168.1.100	00-04-5a-82-96-9f	Ethernet	☐

图5－40：DHCP活动IP表

Local MAC Address（本地MAC地址）：这里显示路由器的LAN（局域网）接口MAC地址。

IP Address（IP地址）：此处显示路由器的局域网IP地址。

Subnet Mask（子网掩码）：此处显示路由器的子网掩码。

DHCP Server（DHCP服务器）： 如果路由器用作DHCP服务器，将会在此处显示。

DHCP Client Table（DHCP客户端表）：点击 "DHCP Clients Table" 按钮来浏览路由器已分配IP地址的电脑列表。 "DHCP ACTIVE IP Table" （DHCP活动IP表）页面列出了DHCP服务器IP地址、客户端主机名，IP地址和MAC地址。如要删除一个DHCP客户端，勾选信息旁边的复选框，然后点击 "Delete" 按钮。点击 **"Refresh"** 按钮，更新信息。

点击 **"Refresh"** 按钮，更新屏幕上的信息。

附录 A：故障处理

这个附录由两个部分组成“一般问题与解决方法”和“常见问题”。这里提供在安装和设置路由器时遇到问题的可能解决方法，如果您的情形如这里所描述的，采用相应的解决办法，问题应该可以解决。如果仍不能解决您的问题，您可以到 www.linksys.com 找寻进一步的答案。

一般问题与解决方法

1. 我需要在计算机上设置一个静态 IP 地址。

使用 DHCP 服务器的路由器 IP 地址的缺省值范围是 192.168.1.100 到 192.168.1.150。设置静态 IP 地址，您只能使用两个范围：196.168.1.2 到 192.168.1.99，以及 192.168.1.151 到 192.168.1.254。使用 TCP/IP 的计算机或网络设备必须设置一个自己单独的识别地址，否则，Windows 会产生 IP 冲突的错误信息。按下列步骤设置 IP 地址：

对于 Windows95，98，和 Me：

A. 点击“开始”，“设置”，和“控制面板”。双击“网络”。

B. 在“已经安装下列网络组件”对话框中选择您以太网适配器相联系的 TCP/IP 。如果您只安装了一台以太网适配器，只能看到没有连接以太网适配器的 TCP/IP 栏。点亮该栏再点击“属性”按钮。

C. 在“TCP/IP 属性”窗口，选择 IP 地址标签，再选择“指定 IP 地址”，输入一个路由器上其他用户没有的 IP 地址，范围是 196.168.1.2 到 192.168.1.99，或者 192.168.1.151 到 192.168.1.254。注意确保每台计算机或网络设备的 IP 地址是唯一的。

D. 点击“网关”标签，在“添加网关”提示中输入路由器的缺省 IP 地址 192.168.1.1。然后点击“添加”按钮接受网关。

E. 点击 DNS 标签，确保已经选择了 DNS。输入主机名和域名，再输入您的 ISP 提供的 DNS 地

址。若没有提供，请与 ISP 联系或登陆网站。

F. 点击“TCP/IP 属性”窗口中的 OK 按钮，再点击网络窗口中的“关闭”或“确定”按钮。

G. 如有需要请重启计算机。

对于 Windows 2000：

A. 点击“开始”，“设置”，和“控制面板”。双击“网络连接”。

B. 点击与您正在使用的以太网相联系的“本地连接”，然后选择“属性”。

C. 在“此连接使用下列项目”框中加亮“Internet 协议（TCP/IP)，然后点击“属性”按钮，接着选择“使用下列 IP 地址”。

D. 输入一个路由器上其他用户没有的 IP 地址，范围是 196.168.1.2 到 192.168.1.99，或者 192.168.1.151 到 192.168.1.254。

E. 输入子网掩码，255.255.255.0。

F. 输入缺省网关，192.168.1.1（路由器的缺省 IP 地址）。

G. 在接近窗口底端选择“使用下列 DNS 服务器”，输入“首选 DNS 服务器”和“备用 DNS 服务器”（有您的 ISP 提供）。请与 ISP 联系或登陆网站。

H. 点击“TCP/IP 属性”窗口中的“确定”按钮，再点击“本地连接属性”窗口中的“确定”按钮。

I. 如有需要请重启计算机。

对于 Windows NT 4.0：

A. 点击“开始”，“设置”，和“控制面板”。双击“网络”。

B. 点击“协议”标签，双击“TCP/IP 协议”。

C. 窗口出现后确保您为以太网选择了正确的适配器。

D. 选择“指定 IP 地址”，输入一个路由器上其他用户没有的 IP 地址，范围是 196.168.1.2 到

192.168.1.99，或者 192.168.1.151 到 192.168.1.254。

E. 输入子网掩码，255.255.255.0。

F. 输入缺省网关，192.168.1.1（路由器的缺省 IP 地址）。

G. 点击“DNS”标签，输入主机名和域名。点击“DNS 搜索顺序”下面的“添加”按钮。在“DNS 服务器”栏输入 DNS IP 地址。ISP 给您的其它 DNS IP 地址按以上方式重复进行即可。

H. 点击“TCP/IP 属性”窗口中的“确定”按钮，再点击网络窗口中的“关闭”或“确定”按钮。

I. 如有需要请重启计算机。

对于 Windows XP：

以下步骤假定您使用的是 Windows XP 缺省界面。如果您使用的是传统的界面（图标和菜单像 Windows 先前版本），请遵循 Windows 2000 中的说明。

A. 点击“开始”和“控制面板”。

B. 点击“网络连接”图标。

C. 点击与您正在使用的以太网相联系的“本地连接”，然后选择“属性”。

D. 在“此连接使用下列项目”框中加亮“Internet 协议（TCP/IP）”，然后点击“属性”按钮。

E. 输入一个路由器上其他用户没有的 IP 地址，范围是 196.168.1.2 到 192.168.1.99，或者 192.168.1.151 到 192.168.1.254。

F. 输入子网掩码，255.255.255.0。

G. 输入缺省网关，192.168.1.1（路由器的缺省 IP 地址）。

H. 在接近窗口底端选择“使用下面 DNS 服务器地址”，输入“首选 DNS 服务器” 和“备用 DNS 服务器”（由您的 ISP 提供）。请与 ISP 联系或登陆其网站获取更多信息。

I. 击“TCP/IP 属性”窗口中的“确定”按钮，再点击“本地连接属性”窗口中的“确定”按

钮。

2. 我要测试我的 Internet 连接

A. 检查您的 TCP/IP 设置

如果您不知道应该怎么做，请参考“附录 D：Windows 帮助”。

B. 打开一个命令行提示

对于 Windows 98/ME

点击“开始”菜单中的运行。在打开的窗口，输入“Command”，按回车键或者点击确定。

对于 Windows 2000/XP

点击“开始”菜单中的运行。在打开的窗口，输入“Cmd”，按回车键或者点击确定。

C. 在命令提示符下，输入“ping 192.128.1.1”按下回车键。

如果获得响应，则这部计算机连接到了路由器。

如果没有响应，请检查电缆，且确认在您的以太网适配器的设置中选中自动获取 IP 地址。

D. 在命令行提示符下，输入“ping”后面跟着您的 Internet 或者 WAN IP 地址，再按 Enter 键。

这个 Internet 或者 WAN IP 地址可以在路由器的网页设置的状态页中看见。

· 如果您获得响应，则这台计算机连接到路由器。

·如果没有响应，则在其他的计算机上试试 ping 命令，以确定是否是您的主机出了问题。

E. 命令行提示符下，输入“ping www.yahoo.com” ，再按 Enter 键。

· 如果您获得响应，则这台计算机连接到 Internet。

·如果没有响应，则在其他的计算机上试试 ping 命令，以确定是否是您的主机出了问题。

3. 我不能通过路由器获得 Internet 连接

A. 参考“问题 2。我要测试我的 Internet 连接”，确定您有正确的连接

B. 如果您需要向您的 ISP 注册您的以太网适配器的 MAC 地址，请参看“附录 C： 为以太网适配卡查找 MAC 地址和 IP 地址”。如果您需要复制您的以太网适配 MAC 地址到路由器上，请参看“第六章：使用路由器的基于网页的工具”部分获得更多细节。

C. 确认您使用正确的 Internet 设置。联系您的 ISP，以确定您的以太网连接类型：DHCP，固定 IP，或者 PPPoE（通常为 DSL 用户使用)。请参看“第六章：使用路由器的基于网页的工具”部分获得更多 Internet 连接设置细节。

D. 确认您有一条正常的电缆线。检查 Internet 指示灯是否一直亮着。

E. 确认您已经把您的电缆或 DSL 调制解调器连接到路由器的 Internet 口。确定在路由器的配置网页中的状态页面显示了从您的 ISP 获得的有效 IP 地址

F. 关闭计算机，路由器和电缆/DSL 调制解调器。等 30 秒后，然后打开计算机，路由器和电缆/DSL 调制解调器。查看路由器的配置网页中的状态页面，看您是否获得了一个 IP 地址。

4. 我不能进入路由器的网页配置工具中的设置页面

A. 参考“问题 2。我要测试我的 Internet 连接”，确定您的计算机正确连接到路由器。

B. 请参看“附录 C： 为以太网适配卡查找 MAC 地址和 IP 地址”以确认您的计算机配置好 IP 地址，子网掩码，网关和域名服务器。

C. 设置一个固定 IP 地址

D. 参看问题“10 我要删除代理设置或者拨号上网的弹出窗口（PPPoE 用户)”

5．我不能让我的虚拟专用网络（VPN）通过路由器正常工作。

打开路由器的基于网页的工具，如“第六章：使用路由器的基于网页的工具”所示，进到 Security 选项的 VPN 页面。确定您已经允许 IPSec 和/或 PPTP 通过

使用带 ESP（Encapsulation Security Payload 知名的协议 50）认证的 IPSec 的 VPN 会工

作得很好。至少有一个 IPSec 连接通过路由器工作；然而，相似的 IPSec 连接可能依赖于您的 VPN 设置。

使用 IPSec 和 AH（Authentication Header 知名的协议 51）的 VPN 是与路由器兼容的。AH 由于与 NAT 标准存在偶然的不兼容性而有限制。

改变路由器的 IP 地址到另一个子网段以避免 VPN IP 地址和您的局域网 IP 地址的冲突。例如，如果您的 VPN 服务器制定一个 IP 地址 192.168.1.X（X 是从 1 到 254 的一个数）和您的网络 PC 的 IP 地址是 192.168.1.X（X 是和 VPN IP 地址使用相同的数），路由器把资料路由到正确的位置将存在困难。如果您改变路由器的 IP 地址为 192.168.2.1，就可以解决问题。通过基于网页工具中的 Setup 选项改变路由器的 IP 地址。如果您为网络上的任何计算机或者网络设备指定固定 IP 地址，您需要根据 192.168.2.Y（Y 是 1 到 254 的任何数字）改变 IP 地址。注意在网络里每个 IP 地址必须是唯一的。

您的 VPN 可能需要把端口 500/UDP 的数据包传递给连接到 IPSec 服务器的计算机。参考问题“7. 我需要设置在线游戏主机或者使用其他 Internet 应用程序“获得更多细节。

请浏览 Linksys 主页获取更多资料 www.linksys.com

6．我要在路由器后面架设一个服务器。

想要使用网页，FTP 或者邮件服务器，您需要知道它们相应使用的端口号。例如，端口号 80（HTTP）为网页服务器使用，端口号 21 为 FTP 服务器使用，端口号 25（SMTP 发送）和端口号 110（POP3 接收）为邮件服务器使用。您可以浏览由您所安装的服务器提供给您的文档获得更多信息。　按照以下步骤通过路由器的网页配置工具设置端口。我们可以安装网页，FTP 和邮件服务器。

A．输入 http://192.168.1.1 或者路由器的 IP 地址访问路由器的配置页面。转到“Application&Gaming”页中的“Port Forwarding”选项。

B．为您要使用的用户程序输入一个名字。

C．输入您使用的服务的扩展端口范围。例如网页服务器的端口范围为 80－80。

D．选择您使用的协议，TCP 或/和 UDP。

E．输入您想要端口服务器要用的 PC 或者网络设备的 IP 地址。例如，如果网页服务器的 IP 地址为 192.168.1.100，则您需要输入 100。请参看“附录 C： 为以太网适配卡查找 MAC 地址和 IP 地址”以获取您的计算机的 IP 地址。

F．选中您要使用的端口服务的端口“Enable”选项。如以下例子所示：

用户程序	扩展端口	协议	IP 地址	Enable
网页服务器	80－80	Both	192.168.1.100	X
FTP 服务器	21－21	TCP	192.168.1.101	X
SMTP（发送）	25－25	Both	192.168.1.102	X
POP3（接收）	110－110	Both	192.168.1.102	X

完成配置后点击“Apply”按钮，然后点击“Continue“按钮。

7．我需要设置在线游戏主机或者使用其他 Internet 应用程序

如果您需要玩在线游戏或者使用 Internet 应用程序，不需要做任何端口映射或者设置 DMZ 主机，大多数都能正常工作。但可能有些例外情况。这将要求您设置路由器以传送输入数据包或数据到指定计算机。使用 Internet 应用程序也与这相似。获得使用的端口服务信息的最好办

法是到您使用的在线游戏或者应用程序的网站查询。按照以下步骤设置在线游戏主机或者使用一些 Intrnet 应用程序：

A. 输入 http://192.168.1.1 或者路由器的 IP 地址访问路由器的配置页面。转到"Application&Gaming"页中的"Port Forwarding"选项。

B. 为您要使用的用户程序输入一个名字。

C. 输入您使用的服务的扩展端口范围。例如，您想设置一个网页服务器，则输入端口范围 80－80。

D. 选择您使用的协议，TCP 或/和 UDP

输入您想要端口服务器要用的 PC 或者网络设备的 IP 地址。例如，如果主机的 IP 地址为 192.168.1.100，则您需要输入 100。请参看"附录 C：为以太网适配卡查找 MAC 地址和 IP 地址"以获取您的计算机的 IP 地址。

E. 选中您要使用的端口服务的端口"Enable"选项。如以下例子所示：

用户程序	扩展端口	协议	IP 地址	Enable
UT	7777－27900	Both	192.168.1.100	X
Halflife	27015－27015	Both	192.168.1.105	X
任何 PC	5631－5631	UDP	192.168.1.102	X
VPN IPSec	500－500	UDP	192.168.1.100	X

完成配置后点击"Save Settings"按钮。

7．Internet 游戏，服务器或者应用程序不能正常工作

如果您碰到 Internet 游戏，服务器或者应用程序功能障碍，确认将您的一部 PC 以 DMZ 方式向 Internet 公开。当一个应用程序需要用到太多的端口或者您不确定哪些端口要使用时，这个选项很有用。如果您想使用 DMZ 方式，请确认关闭所有的映射入口（换句话说，进入路由器的数据首先会被映射设置检查，如果数据进入的端口没有端口映射，则路由器会。将数据发送到那些您设置为 DMZ 方式的 PC 或者网络）。按照以下步骤设置 DMZ 方式

A．输入 http://192.168.1.1 或者路由器的 IP 地址访问路由器的配置页面。转到"Application&Gaming"页中的"Port Forwarding"选项。

B．关闭或者删除您为映射输入的入口，保留这些资料以便今后您需要使用。

C．转到"Application&Gaming"页中的"DMZ"选项。

D．选中"DMZ"的"Enable"项。在 DMZ 主机 IP 地址区，输入您想要向 Internet 公开的计算机 IP 地址。这将屏蔽该机 NAT 技术。请参看"附录 C：为以太网适配卡查找 MAC 地址和 IP 地址"以获取您的计算机的 IP 地址。

完成配置后点击"Save Settings"按钮

9．忘了密码或者当我保存设置到路由器时总是提示输入密码。

按住路由器的 Reset 键 10 秒，然后放开，将路由器恢复出厂设置。如果您保存设置时仍然提示输入密码，则执行以下步骤：

A．输入 http://192.168.1.1 或者路由器的 IP 地址访问路由器的配置页面。输入缺省密码"admin"，点击"Administrations"页中的"Management"标签。

B．在路由器密码区输入，输入另一个密码，在下一个位置输入相同的密码以确认

点击"Save Settings"按钮。

10．我是一个 PPPoE 用户，我要删除代理设置或者拨号上网的弹出窗口

如果您的计算机使用了代理设置，请需要关闭它。因为路由器是作为 Internet 连接的网关，计算机不需要任何代理就可以访问。请按以下向导确认您没有使用任何代理设置且您的浏览器是直接连接到网络。

对于 IE5.0 或者更高版本

A． 点击“开始”菜单，“设置”中“控制面板”标签。双击 Internet 标签。

B． 点击“连接”页

C． 点击“局域网设置”，删除任何选中标签

D． 点击“确定”回到前一页

E． 点击标签“从不进行拨号连接”。这将为 PPPoE 用户删除任何拨号上网，POP 上网设置。

如果是 Netscape4.7 或者更高版本

A． 启动“Netscape Navigator”，点击“编辑”，“选项”，“高级”和“代理”

B． 确定这也中您是直接连接到 Internet。

关闭所有窗口结束。

11．我要设置路由器到出厂设置重头开始

按住路由器的 Reset 键 10 秒，然后放开。这将路由器恢复到出厂时密码，端口映射和其他选项的缺省设置。换句话说，路由器回到了原始的出厂配置。

12．我要升级固件

为了升级固件以拥有最新功能，您需要到 Linksys 的网站 www.linksys.com 下载最新的固件

升级文件。按照以下步骤：

A. Linksys 的网站 www.linksys.com 下载最新的固件升级文件。

要升级固件，请按照“第五章：使用路由器的基于网页的工具”或者“附录 B：固件升级”中升级部分步骤去做。

12．固件升级失败

很多原因会使升级失败。按照以下步骤升级固件：

A． 如果固件升级失败，使用 TFTP 程序（和固件升级文件一起下载的）。打开和 TFTP 程序与固件升级文件一起下载的 PDF 文档，按照 PDF 文档的指令做。

B． 在 PC 上设置静态 IP 地址。参考“问题 1：我需要在计算机上设置一个静态 IP 地址。”将您的计算机设置以下的 IP 地址配置：

IP 地址：192.168.1.50

子网掩码：255.255.255.0

网关：192.168.1.1

C． 使用 TFTP 程序或者路由器基于网页的工具“Administration”标签中的“Firmware Upgrade”页面升级固件。

13．我的 DSL 服务器的 PPPoE 总是不能连接

PPPoE 实际上不是一个传输或者总是打开的连接。DSL ISP 在非活动期间会断开服务，就像普通的电话拨号上网一样。有一个设置选项保持活动连接。这并非总是有用，所以您需要周期性的重新建立连接。

A. 打开网页浏览器，输入 http://192.168.1.1 或者路由器的 IP 地址访问路由器的配置页面，连接路由器。

B. 如果需要，输入密码（缺省密码是 admin）

C．在设置页面，选择“Keep Alive”选项，然后设置重新拨号周期为 20 秒

D． 点击“Save Settings”按钮。

E．点击“Status”页，点击“Connect”按钮。

F．您可以看到登录状态显示为正在连接。按 F5 键刷新屏幕，直到您看见登陆状态显示为已经连接。

如果连接又丢失，按 A—F 步骤重新建立连接。

14．我不能访问我的 Email，网页或者我从 Internet 收到被破坏的数据

可能最大传输单元（MTU）需要调整。缺省 MTU 为 1500，对于大多数 DSL 用户，强烈推荐使用 MTU 为 1492。如果您有问题，执行下列步骤：

A. 打开网页浏览器，输入 http://192.168.1.1 或者路由器的 IP 地址访问路由器的配置页面，连接路由器。

B. 如果需要，输入密码（缺省密码是 admin）。

C. 找到“MTU”选项，选择“Manual”，在“Size”区输入 1492

D. 点击“Save Settings”按钮继续。

如果您改变 MTU 的值仍有问题，试试下列值，一次一个，按下述顺序，直到您的问题解决：

1462

1400

1362

1300

15．我要使用端口触发

端口触发用于外向端口服务，会触发路由器打开一个指定端口，具体由 Internet 应用程序

使用的哪个端口而定。按照下列步骤：

A. 打开网页浏览器，输入 http://192.168.1.1 或者路由器的 IP 地址访问路由器的配置页面，连接路由器。

B. 如果需要，输入密码（缺省密码是 admin）。

C. 点击 “Application&Gaming” 页中的 “Port Triggering” 标签。

D. 为您需要使用的应用程序输入任意名字。

E. 输入触发端口范围的开始和结束端口。从您的 Internet 应用程序供应商那里获取关于它用到哪些外向端口服务的更多信息。

17．当输入 URL 或 IP 地址，出现超时错误或者提示重试

·先检查其他计算机是否正常工作，如果它们正常工作的话，再确定您的计算机网络设定是否正确（IP 地址，子网掩码，缺省网关，和 DNS）。重新启动您的计算机。

·如果计算机都配置正确，但还是不能正常工作。请检查您的路由器。确保它已经上电并已经连接正确。进入它，并检查设置。(（假如您不能进入，请检查网络以及电源线连接正确)。

·如果路由器连接正确，请检查 Internet 连接（DSL/Cable Modem）是否正确，

·按您的 ISP 提供的信息来手动配置有 DNS 的 TCP/IP。

·确定您的网络浏览器设置没有使用拨号连接而是直接连接 Internet，如果是 IE，请点击 “工具”，“Internet 选项”，再进入“连接”选项页面，确保设置在“不使用拨号连接”。如果是 Netscape Navigator，请点击 “编辑”，“选项”，“高级”，“代理服务器”，确保设置在 “直接连接 Internet”。

常见问题

什么是 MIB?

MIB（管理信息库）是一个和管理路由器的第三方 SNMP 软件协同工作的数据文件，要使用 MIB 文件和第三方 SNMP 软件协同工作，按照来自第三方的 SNMP 软件的指导。MIB 数据文件将在 Linksys 的主页可用：www.linksys.com

我可以使用带 BEFVP41 的其他路由器的固件吗?

不行。如果您企图使用其他路由器的固件，您可能损坏路由器。仅仅使用专门写的发表在 Linksys 主页上的固件：www.Linksys.com

什么是 SNMP?

SNMP（简单网络管理协议）它是使用最广的网络操作控制协议。文件资料从 SNMP 主体传送到监察网络工作站的控制台。这些 SNMP 主体包括硬件或者是反映网络设备运作的软件。主体用 MIB 返回信息，该信息结构确定设备中哪些是可以获取的，哪些是可以控制的。参考“附录 G：SNMP 功能”。

这台路由器可以支持多少个 IP 地址?

这台路由器最多可以支持 253 个 IP 地址。

这台路由器是否支持 IPSec 数据包通过?

是的，它是路由器的内建功能，路由器自动启动。

路由器应该安装在网络的哪个地方?

在一个典型环境下，路由器安装在调制解调器与局域网之间，把路由器电缆插在调制解调器的以太网端口。

路由器是否支持 IPX 和 AppleTalk?

不支持，TCP/IP 是国际互联网的唯一标准，是全球通信的标准。IPX 和 AppleTalk，可以用于局域网到局域网连接，单不能用于广域网到局域网的连接。

什么是网络地址转换（NAT）？ 其作用是什么?

网络地址转换可以把多个内部局域网的 IP 地址转换为一个国际互联网的 IP 地址。这样增加安全层次，因为局域网上计算机的地址不在国际互联网上发送，此外，NAT 允许路由器用于低费用的国际互联网帐户，在这里只需有 ISP 提供一个 IP 地址，在此 IP 地址后面，用户可以有很多局域网 IP 地址。

除了 windows98/ME/2000/XP 外，是否还支持其他操作系统?

是的，会支持。但是 Linksys 目前不为非 Windows 操作系统的安装，配置或故障处理提供专用技术支持。

这台路由器是否支持用 ICQ 传送?

是的，您可以用下列步骤，点击 ICQ 的 menu－>preference->connection Tap->,然后在 “I am behind a firewall or proxy” 划上勾。然后将防火墙超时时间设置为 80 秒。这样，在 Internet 上的用户就可以把文件传送到路由器后的用户。

我安装了一个虚拟的竞赛服务器，但 LAN 上其它用户不能加入。我该怎么办?

假如您可以运行专用虚拟竞赛服务器，请在服务器 IP 地址中为每一台 LAN 计算机和传送端口

7777，7778,7779，7780,7781,和 27900 分别创立一个静态 IP 地址。您也可以使用端口传送范围 7777 到 27900。如果使用 UT Server Admin，传送另一个端口（8080 通常性能很好，但只用于远程管理。您也可以中断它。)，并且在 server.ini 文件的[U Web.WebServer]部分，将 ListenPort 设置成 8080，以及将 ISP 告诉您的路由器 IP 输入到 ServerName 上即可。

LAN 的多名游戏者能否进入同一游戏服务器并使用同一公共 IP 地址同时玩呢?

这要取决于您使用的是哪种网络游戏或游戏服务器的类型。例如，Unreal Tournament 支持一个公共 IP 下多个登录。

如何使 Half-Life:Team Fortress 与路由器一同运行?

Half-Life 的客户端口缺省是 27005。您 LAN 上的计算机需要将“+Clientport 2700x”添加到 HL 快捷方式命令栏内；其中 x 可以是 6，7，8 或更大的数。这样可以使多台计算机连接到同一服务器上。请注意：1.0.1.6 版本不允许具有相同 CD 密码的多台计算机相连，即使是在同一 LAN 上（1.0.1.3 没有此类问题）。主机管理游戏时，HL 服务器无需在 DMZ 上，可以把端口传送到计算机服务器的 IP 地址上。

我如何能阻止不正确的 FTP 下载?

如果您 FTP 用户端软件无法正确下载，请换另一个 FTP 软件。

网络页面中止，下载数据被破坏或者显示屏出现的都是乱码，我该怎么办?

把您的以太网强制调节成 10Mbps 模式或半双工模式，关掉以太网适配器上的“Auto-negotiate”特性。这是临时方案。(请在您的以太网适配器的高级属性标签里找到）确保浏览器里的代理设置已经中断。详情可登录 www.linksys.com。

如果安装失败该怎么办?

按住 Reset 按钮直到 Diag 指示灯亮了又熄灭就可以重新设置路由器。通过关闭装置电源再开启重置您的 Cable/DSL modem。从 Linksys 网站 www.linksys.com 获取并使用最新固件。

如何通知我新的路由器固件升级?

在 www.linksys.com 上会更新 Linksys 固件升级版本，可以免费下载。路由器固件可以用 TFTP 程序升级。如果路由器的 Internet 连接运行正常，无需下载新的固件版本，除非您向使用其中某些新的功能。下载新的版本并不会提高 Internet 连接的质量或速度，相反，可能会影响您当前连接的稳定性。

路由器在 Macintosh 环境下是否能正常运行?

是的，但是路由器的安装页面只有在 Internet Explorer4.0 或 Netscape Navigator4.0 或更高版本中才有效。

我无法进入路由器的网路配置屏幕。该怎么办?

您可以先删除 Internet 浏览器上的代理设置，例如 Netscape Navigator 或 Internet Explorer。或者删除浏览器上拨号上网设置。查看您的浏览器文档，确保浏览器连接正确，任何拨号上网都已中断。对于 Internet Explorer，点击“工具”，“Internet 选项”，然后是“连接”标签，确保 Internet Explorer 设置在“从不进行拨号连接”。对于 Netscape Navigator 而言，点击“编辑”，“选项”，“高级”和“代理服务器”。确保您的 Netscape Navigator 设置为“直接连接到 Internet”。

什么是 DMZ Hosting?

Demilitarized Zone (DMZ) 允许一个 IP 地址暴露在 Internet 上。有些程序要求打开多个 TCP/IP 端口。若您想使用 DMZ Hosting，建议给计算机设置一个静态 IP 地址。LAN IP 地址的获取请参照

“附录 C: 查找网络适配器的 MAC 地址和 IP 地址。”

使用 DMZ Hosting 是，被暴露的用户能否与路由器共享同一个公共 IP?

不行。

路由器能否传送 PPTP 封包或活跃地传送 PPTP 会话?

路由器允许 PPTP 数据包通过。

路由器与平台是否兼容?

只要支持以太网或 TCP/IP 的平台就与路由器兼容。

可以同时传送多少端口?

理论上路由器同时可以建立 520 个话路，但您只能同时传送 10 个端口。

路由器可以取代调制解调器吗? 路由器里是否带有 Cable/DSL modem?

不能，这个版本的路由器必须和 Cable/DSL modem 一起运行。

哪些 modem 与路由器兼容?

这款路由器实质上与任何支持以太网的电视电缆/DSL 调制解调器兼容。

如何确定我是否有静态或 DHCP IP 地址?

请与您的 ISP 联系获取这些资料。

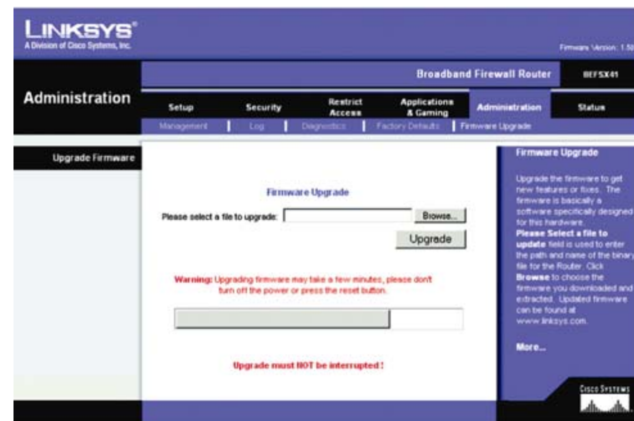
我如何让 mIRC 与路由器一起正常工作?

在 Port Range Forwarding 标签下，将那台使用 mIRC 的计算机的端口传送设置成 113。

如果您有任何问题不能在这里找到，请访问 Linksys 网站 www.linksys.com

附录 B：升级固件

您可以使用路由器的基于网页的工具升级固件；但是您要是这么做，可能就会丢失原来在这台路由器配置过的设置。



图B—1：升级固件

按照以下步骤升级路由器的固件：

1. 从 Linksys 的网站 www.linksys.com 下载固件升级文件。
2. 解压文件到您的计算机上。
3. 在路由器网页工具点击 Administration 标签，然后点击 “Update Firmware” 标签。
4. 在升级固件页面，输入固件升级文件的位置，或者点击 “Browse” 按钮找到该文件。
5. 然后点击 “Upgrade” 按钮，按照页面提示去做。

附录 C：为您的以太网卡查找 MAC 地址和 IP 地址

本章教您如何在 PC 上找到您的以太网适配卡的 MAC 地址和 IP 地址，这样您就可以使用路由器的 MAC 过滤和/或者 MAC 地址复制功能。您也可以找到您的计算机的以太网卡地址。这个 IP 地址用于路由器的过滤，映射和/或者 DMZ 功能。按照这个附录的下列步骤在 Windows 98，Me，2000 或者 XP 系统查找以太网卡的 MAC 地址和 IP 地址。

Windows 98 或者 Windows ME 系统

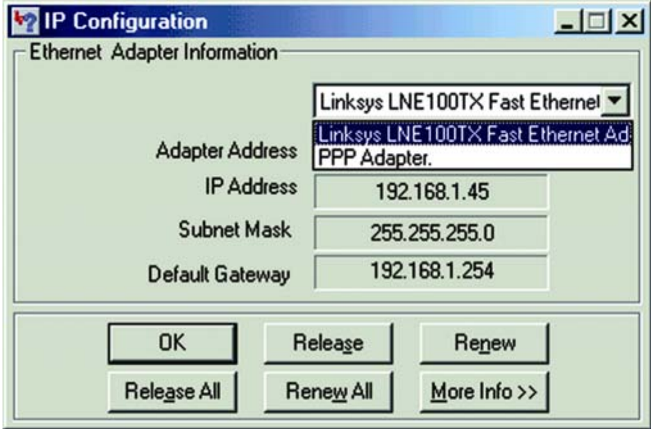
1. 点击 “开始” 和 “运行”。在打开的栏内输入 “winpcfg”。然后敲回车键或点击 “确定” 按钮。
2. 当出现了 “IP 配置 “窗口后，选择通过五类非屏蔽双绞线连接到路由器的以太网适配器。
3. 记下计算机屏幕显示的网络适配器。这时您的以太网适配器的 MAC 地址，呈现出一系列的数字和字母。

MAC 地址/适配器地址会用于 “MAC 过滤” 或者 “MAC 地址复制”。

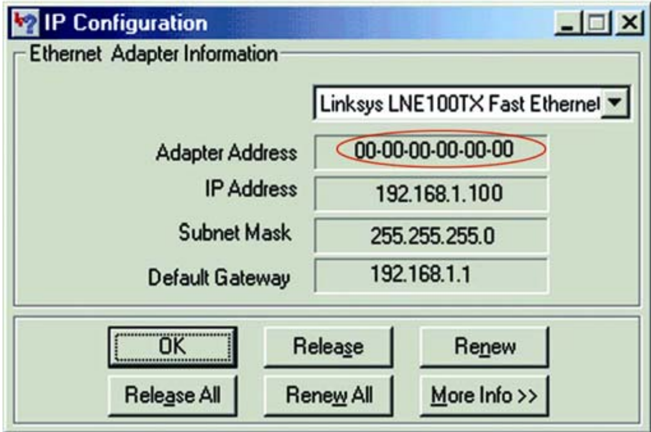
例子显示了您的以太网适配器的 IP 地址是 192.168.1.100。但您的计算机显示的可能有所不同。



请注意：MAC 地址也叫做适配器地址。



图C－1：IP配置页面



图C－2：MAC地址/适配器地址

对于 Windows 2000 和 XP：

1. 点击“开始”和“运行”。在打开的栏内输入“cmd”。敲回车键或点击“确定”按钮。在命令指示符中，输入 ipcongfig/all。然后敲回车键。

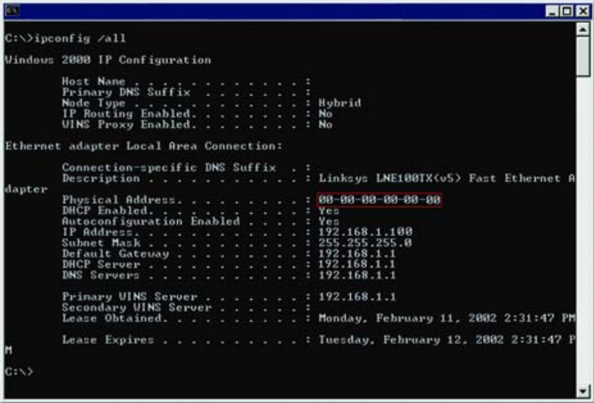
2. 记下屏幕上显示的物理地址；这就是您的以太网适配器的 MAC 地址，呈现出一系列的数字和字母。

MAC 地址/适配器地址会用于“MAC 过滤”或者“MAC 地址复制”。

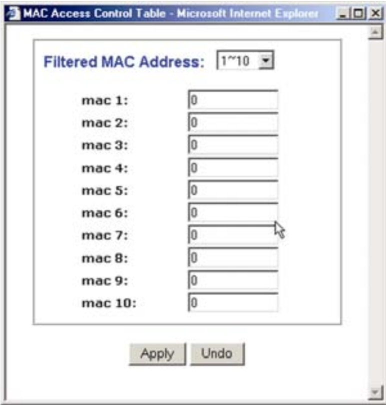


请注意：MAC 地址也可称作物理地址。

例子显示了您的以太网适配器的 IP 地址是 192.168.1.100。但您的计算机显示的可能有所不同。



图C－3：MAC地址/适配器地址



图C－4：MAC地址过滤

对于路由器基于网页工具

对于 MAC 地址过滤，按这个格式，XXXXXXXXXXXX ，输入 12 位数的 MAC 地址，不用连字符。

对于 MAC 地址复制，在所给 MAC Address 栏输入 12 位数的 MAC 地址，每栏两个数字。



图C－5：MAC地址复制

附录 D：windows 帮助

所有的网络产品都要求微软 Windows 操作系统。Windows 操作系统在世界上使用最广泛，带来许多有助于使网络更加容易使用的特色功能。这些特色功能可以通过 Windows 的帮助或者这个附录里的描述来了解。

TCP/IP

在计算机可以和路由器通信之前，TCP/IP 必须启动。 TCP/IP 是一套指令，或者协议，所有的 PC 通过它与有线或者无线网络通信。要是不启动 TCP/IP，您的 PC 将无法使用网络。Windows 帮助提供了启动 TCP/IP 协议的全程指导。

共享资源

如果您想通过网络共享打印机，目录或者文件，Windows 帮助提供了共享资源的全程指导。

网上邻居

在您的网络上的其他 PC 会显示在网上邻居里。Windows 帮助提供了添加 PC 机到您的网络上的全程指导。

附录 E：最优化 VPN 安全

当您用路由器的防火墙最优化您的网络安全的时候，您也应该用路由器的 VPN 功能最优化您的数据安全。

IPSec 与多数的 VPN 终端兼容，在认证用户省份时确保数据保密和通过认证。对于 IPSec，认证是基于 PC 的 IP 地址。这不仅可以确定用户身份，还可以在网络层建立安全的隧道，保护所有通过的数据。

通过操作网络层，IPSec 独立于任何在网络上跑的应用程序。这种方式，不会损害您的 PC 机性能，而且允许您为了更优的安全性做更多的事情。当然，很重要的是，由于加密和解密数据，IPSec 的加密确实会造成网络吞吐量的稍微下降。

一些 VPN 仍旧保持 IP 头不加密。这些 IP 头包含了 VPN 隧道两头用户的 IP 地址，可能被以后的黑客攻击利用。然而，VPN 路由器，并不会让 IP 头保持不加密状态。使用一种叫做 PFS（Perfect Forward Secrety）的方法，不仅加密 IP 头，而且用于隧道安全的密钥也加密了。

所有的保护的代价实际上比大多数 VPN 终端软件包来得低。VPN 路由器允许在您的局域网的用户保护他们经过互联网的数据的安全性，无须购买其他 VPN 硬件厂商或者软件包需要的额外的客户端许可证。把 VPN 功能交给路由器处理，好过用您的 PC 机处理（这是软件包所需要的），这样可以释放您的 PC 机的资源而去完成更多的功能，效率更高。一个额外的好处是您将不需要重新配置您的局域网上的任何 PC 机。

和 VPN 路由器使您的数据安全一样，还有很多方法去优化安全性。下面是怎样在 VPN 路由器

上提高数据安全性的一些建议：

1．优化您的其他网络的安全性。为您的互联网连接安装防火墙路由器，使用最新的无线网络安全措施。

2．尽可能的减小您的 VPN 隧道的范围。比允许一个范围的 IP 地址更好的方法是对想要的终端指定 IP 地址。

3．不要设置远程安全组为 Any，这样会将 VPN 开放给任何 IP 地址。指定一个 IP 地址。

4．优化加密和认证。尽可能使用 3DES 加密和 SHA 认证。

5．管理好您的预共享密码。经常更换您的预共享密码。

在互联网上的数据传输是经常被忽略的网络安全漏洞。通过优化 VPN，与防火墙路由器和无线安全一起，您就可以保护您的数据安全甚至在它离开您的网络的时候。

附录 F：在 Windows2000 或者 XP 计算机和路由器之间配置 IPSec

介绍

这个文档示范了如何使用预共享密钥在 Microsoft Windows 2000 (or XP) 计算机和宽带 VPN 路由器建立一条安全的 IPsec 隧道的步骤。您可以在 Microsoft 网站找到配置 Microsoft Windows 2000 服务器的详细资料。

Microsoft KB Q252735　　如何在 Windows 2000 配置 IPSec 隧道

http://support.microsoft.com/support/kb/articles/Q252/7/35.asp

Microsoft KB Q257225 - 在 Windows 2000 基本 IPSec 常见故障及处理

http://support.microsoft.com/support/kb/articles/Q257/2/25.asp

环境

在这个附录里提到的 IP 地址和其他细节仅仅做解说目的。

Windows 2000 或者 Windows XP

IP 地址: 140.111.1.2 <= ISP 提供的 IP 地址;这只是一个例子

子网掩码: 255.255.255.0

WAG54G

WAN（广域网）IP 地址: 140.111.1.1 <= ISP 提供的 IP 地址;这只是一个例子

子网掩码: 255.255.255.0

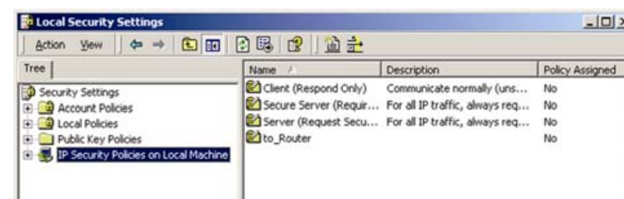
LAN（局域网）IP 地址: 192.168.1.1

子网掩码: 255.255.255.0

如何创建一条安全 IPSec 隧道

步骤 1：创建一条 IPSec 策略

1. 点击 **开始** 按钮, 选择 **运行**, 在打开的窗口输入 **secpol.msc** 本地安全设置窗口就会出现如出现如图：F-1 所示。



图F－1：创建一条IPSec 策略

2. .右键点击 IP Security Policies on Local Computer（本地计算机上 IP 安全策略，对于 WinXp 上） 或者 IP Security Policies on Local Machine（IP 安全策略，在本地机器，对于 win2000)，然后点击 创建 IP 安全策略。

3. 点击 下一步, 然后输入您的策略名（例如, "to_VPNRouter"），然后点击下一步。

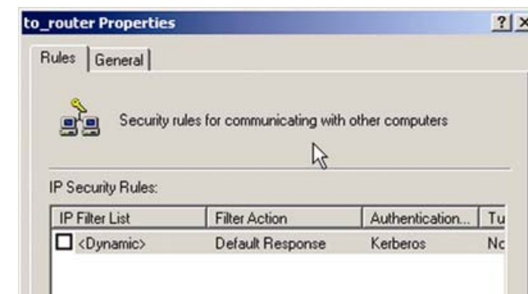
4. 去掉激活默认响应规则 选择框的勾, 然后点击 下一步按钮。

5. 点击完成按钮，确定勾选了编辑选择框。

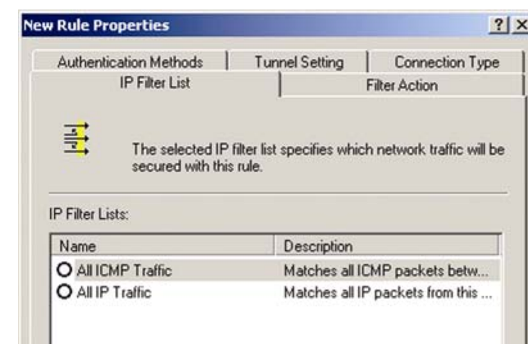
步骤 2：建立过滤器清单: "Win—>路由器" 和 "路由器—>Win" .

[过滤器清单 1]　Win－>路由器

1. 在新策略属性窗口，确认选择了“**规则**”标签，如图 F－2 所示，去除 **使用添加向导** 复选框上的勾,然后点击**添加** 按钮创建一条新规则。

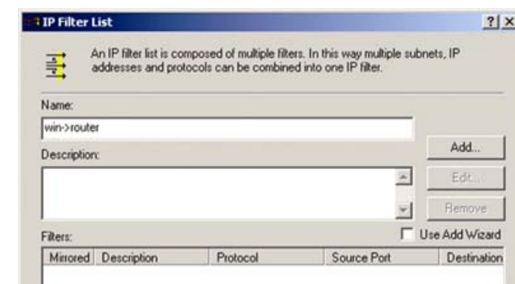


图F－2：新策略属性窗口



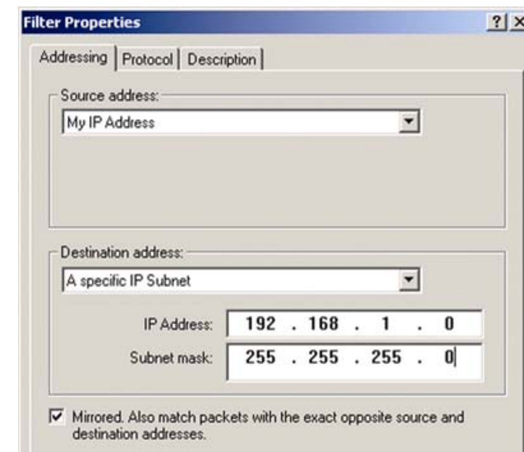
图F－3：IP过滤器清单

3. 确认选择了 IP 过滤器清单标签，点击添加按钮（看图 F－3)。IP 过滤器清单画面就会出现，如图 F－4 所示。给过滤器清单输入一个合适的名字，例如 “Win－>Router”，去除 使用添加向导 复选框上的勾,然后点击 添加 按钮 。



图F－4：IP过滤器清单

4. IP 过滤器清单画面就会出现，如图 F－5 所示，选择**寻址**标签。在**源地址** 栏，选择 **我的 IP 地址**.在 **目的地址**栏，选择 **一个特定 IP 子网**，输入 IP 地址 “192.168.1.0” 和子网掩码 “255.255.255.0” （这些是路由器的缺省设置，如果您改变了这些设置，输入您的新值）。



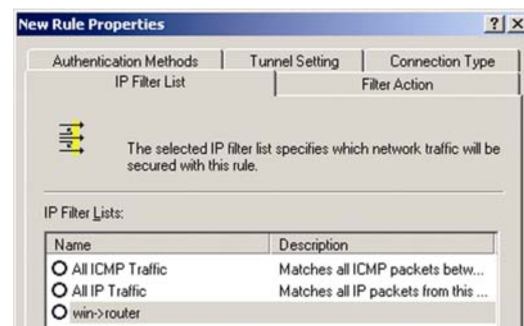
图F－5：寻址标签

5. 如果您要给您的过滤器输入一个描述，点击**描述**标签，在这里输入描述内容。

6. 点击**确定**按钮，然后在 IP 过滤器清单窗口点击确定按钮（对于 WinXP）或者关闭按钮（对于 Win2000）。

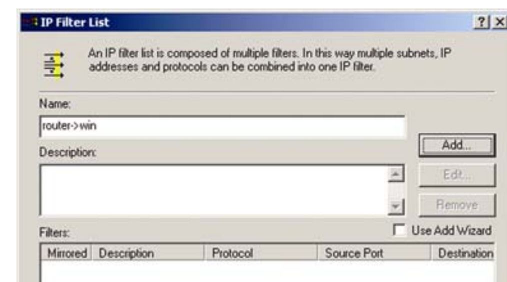
[过滤器清单 2] 路由器－>Win

7. 新规则属性窗口就会出现，如图 F－6 所示。选择 **IP 过滤器清单**标签，确认 **win－>Router** 是选中的，然后点击 **添加** 按钮。



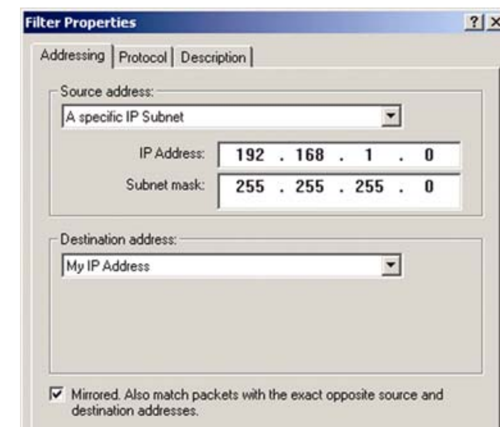
图F－6：新规则属性窗口

8. 给 **IP 过滤器清单**画面应该会出现，如图 F－7 所示。给过滤器清单输入一个合适的名字 “Route**－>Win**”，去除**使用添加向导** 复选框上的勾,然后点击 **添加** 按钮。



图F－7：IP 过滤器清单画面

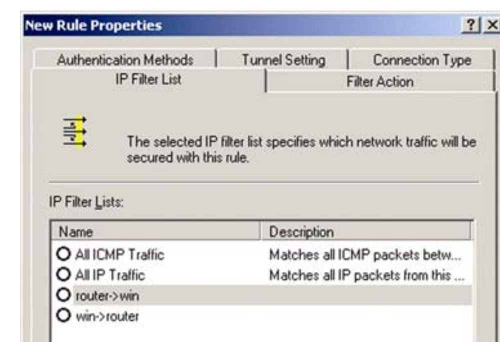
9. IP 过滤器清单画面就会出现，如图 F－8 所示，选择**寻址**标签。在**源地址** 栏，选择**一个特定 IP 子网**，输入 IP 地址 “192.168.1.0” 和子网掩码 “255.255.255.0” （这些是路由器的缺省设置，如果您改变了这些设置，输入您的新值）。在 **目的地址**栏，选择**我的 IP 地址**。



图F－8：寻址标签

10. 如果您要给您的过滤器输入一个描述，点击**描述**标签，在这里输入描述内容。

11. 点击**确定**按钮（对于 WinXP）或者**关闭**按钮（对于 Win2000），IP 过滤器清单画面就会出现，如图 F－9 所示。现在应该列有 “**Win－>** Route” 和 “Route**－>Win**”，点击 IP 过滤器清单窗口的确定按钮（对于 WinXP）或者关闭按钮（对于 Win2000）。

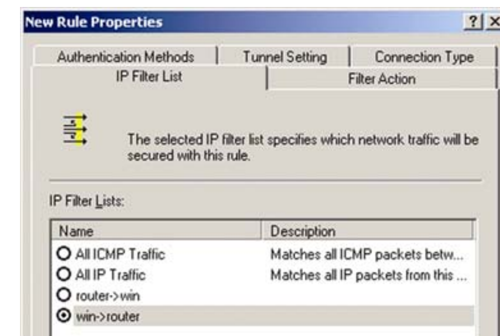


图F－9：IP过滤器清单

步骤 3：配置两隧道的独立规则

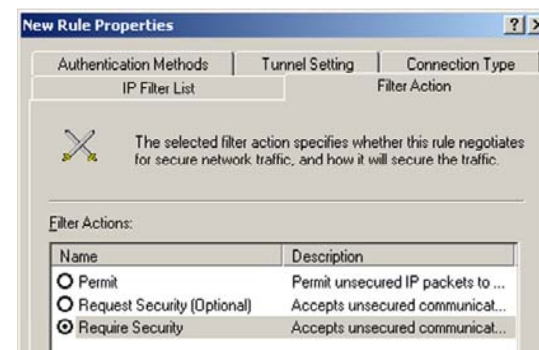
[隧道 1] Win－>路由器

1. 在 IP 过滤器清单标签页，如图 F－10 所示，点击过滤器清单 “Win－>Router” .



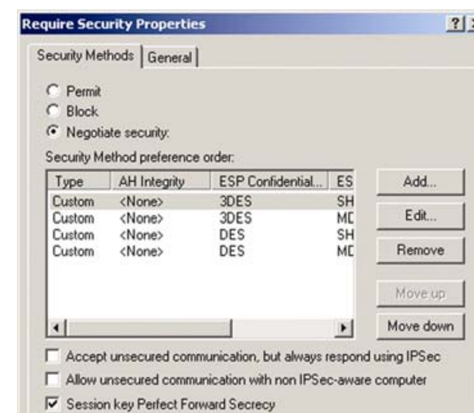
图F－10：IP 过滤器清单标签页

2. 在**过滤操作** 标签页（如图 F－11），点击过滤动作 “要求安全性” 单选框，接着点击 **编辑** 按钮。



图F－11：过滤操作标签页

3. 在安全措施标签页，如图 F－12 所示，确保启动协商安全性选项，去掉接受非安全通信，但总是使用 IPSec 响应复选框的勾。勾选会话密钥完全向前保密 (PFS)选项，然后点击确定按钮。



图F－12：安全措施标签页

4. 选择 认证方法标签页，如图 F－13 所示，点击 编辑 按钮。



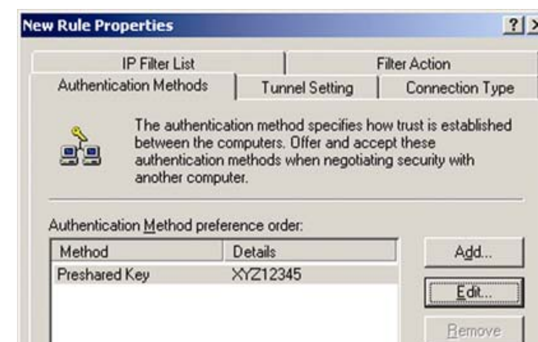
图F－13：认证方法标签页

5. 改变认证措施为 “使用这个字符串来保护密钥交换(预共享密钥)”，如图 F－14 所示，输入预共享密钥字符串，比如 “XYZ123435”，然后点击确定按钮。



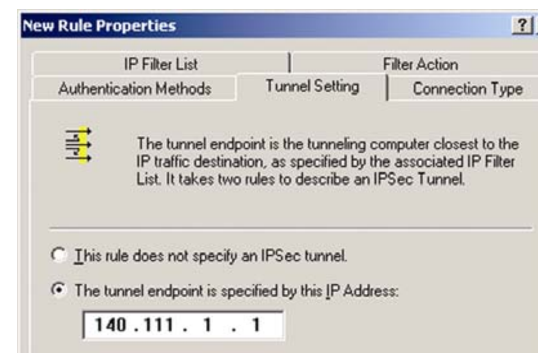
图F－14：认证措施

6．这个新的预共享密钥就会显示在图 F－15。点击 “Apply” 按钮继续，如果它显示在您的页面上，请继续下一步。



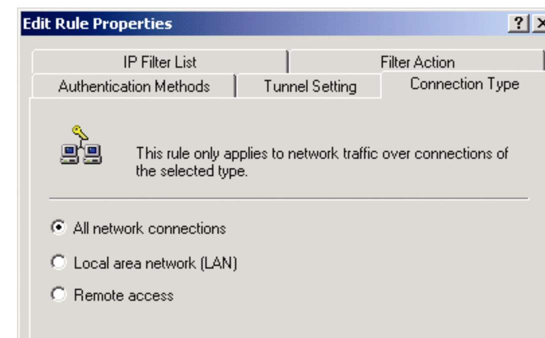
图F－15：预共享密钥

7. 选择 隧道设置标签 ，如图 F－16 所示,选择 隧道终端由这个 IP 地址指定单选框，然后输入路由器的广域网（WAN）IP 地址。



图F－16：隧道设置标签

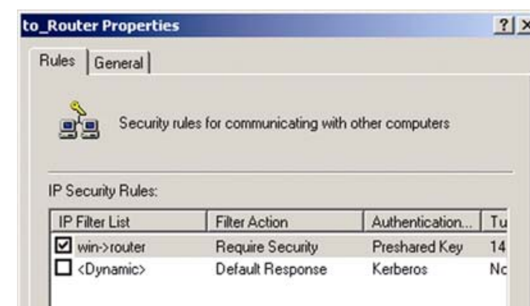
8. 选择连接类型 标签，如图 F－17 所示,点击所有网络连接，然后点击确定 或者 关闭按钮完成这条规则。



图F－17：连接类型标签

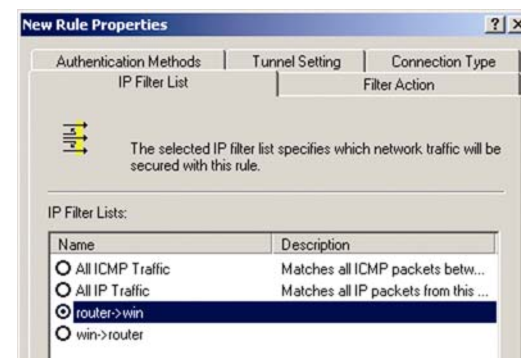
[隧道 2]路由器－>Win

9. 在新策略的属性页面，如图 F－18 所示，确认选择了 “Win－>Router”，去除 使用添加向导 复选框上的勾,然后点击添加 按钮创建第二个 IP 过滤器。



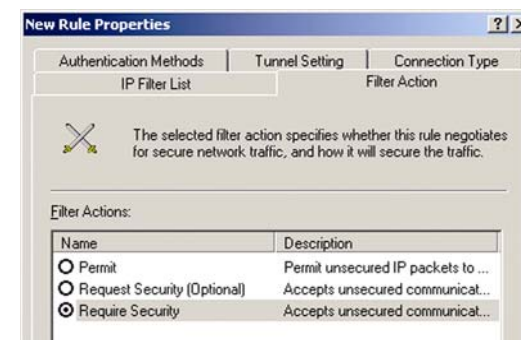
图F－18：新策略的属性

10. 转到 IP 过滤器清单标签页，点击过滤器清单 “Router－>win”，如图 F－19 所示。



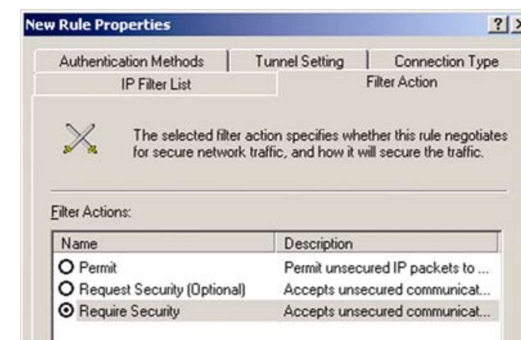
图F－19：IP过滤器清单标签

12. 在**过滤操作**标签页，然后选择过滤操作 **“要求安全性”** ，如图 F－20 所示。然后，点击**编辑**按钮。在**安全措施**标签页，如图 F－12 所示，确保启动**协商安全性**选项，去掉**接受非安全通信，但总是使用 IPSec 响应**复选框的勾。勾选**会话密钥完全向前保密**(PFS)复选框，然后点击**确定**按钮。



图F－20：要求安全性

在 **认证方法** 标签，确认选择了 Kerberos 认证措施，如图 F－21 所示。然后点击 **编辑** 按钮。



图F－21：认证方法标签

13. 改变认证措施为 **“使用这个字符串来保护密钥交换(预共享密钥)”**,输入预共享密钥字符串，比如 “XYZ123435”，如图 F－22 所示。(这是一个简单的密钥字符串。您的密钥应该是唯一但易于记忆的密钥）然后点击确定按钮。



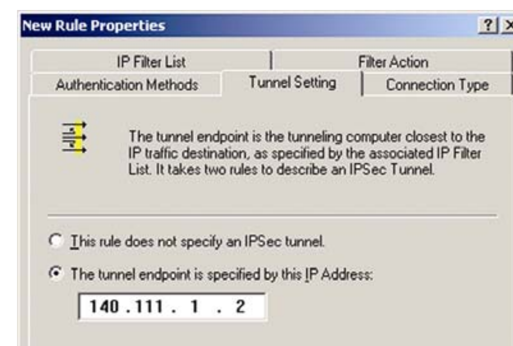
图F－22：改变认证措施

14. 这个新的预共享密钥就会显示在图 F－23。点击 “**Apply**” 按钮继续，如果它显示在您的页面上，请继续下一步。



图F－23：新的预共享密钥

在 **隧道设置**标签，如图 F－24 所示。点选 **隧道终端由这个 IP 地址指定**单选框，然后输入 Windows 2000/XP 计算机的 IP 地址。



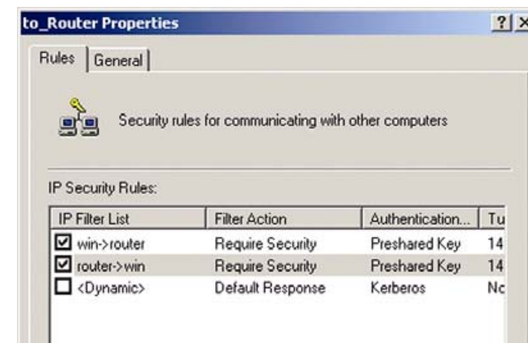
图F-24：隧道设置标签

15. 在**连接类型** 标签,，如图 F－25 所示。选择**所有网络连接**，然后点击**确定**(对于 WinXP)或者 **关闭**(对于 Win2000)按钮完成这条规则。



图F－25：连接类型

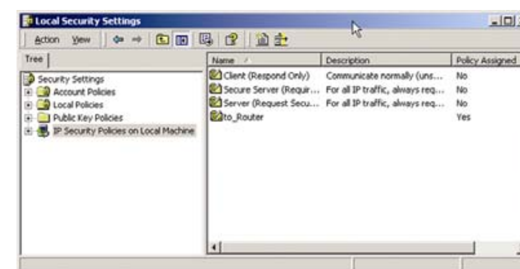
16. 在 **规则**标签，如图 F－26 所示。然后点击**确定**或者**关闭**按钮返回本地安全设置页面。



图F－26：规则标签

步骤 4：指定新的 Ipsec 策略

一个新的绿色箭头出现在文件夹图标中。



图F－27：新的Ipsec策略

步骤 5：通过基于网页工具创建一个隧道

1. 打开您的网页浏览器，在地址栏输入 192.168.1.1，按回车键。

2. 当出现用户名和密码对话框的时候，输入缺省用户名和缺省密码 “admin”，按回车键。

3. 在 Setup 标签，点击 VPN 标签。

4. 在 VPN 标签，如图 F－28 所示，在 “Select Tunnel Entry” 选择隧道项下拉框选择您想要创建的隧道。然后点击 **“Enable”**。在**隧道名字**栏输入隧道名称。这让您识别多个隧道，且不必与隧道另一端使用的名字相匹配。

5. 在 Local Secure Group（本地安全组）栏输入本地 VPN 路由器的 IP 地址和子网掩码想要允许访问整个子网，在 IP 地址栏的最后一位输入 0（例如 192.168.1.0）。

6. 在 Remote Security Router（远程安全路由器）栏输入隧道的另一端的 VPN 设备的 IP 地址和子网掩码（您想与之通信的远程 VPN 路由器或者设备）。

7. 从两种不同加密类型中选择 :DES 和 3DES（推荐您使用 3DES，以获得更大安全性）。您可以选择任何一个，但您必须保证隧道另一端的 VPN 设备也使用相同的加密类型。或者您可选择 “Disable”，不使用加密。

8. 从两种不同认证类型中选择 ：MD5 和 SHA（推荐使用 SHA，以获得更大安全性）。和加密一样，您可以选择其中任何一个，但您必须保证隧道另一端的 VPN 设备也使用相同的加密类型。或者隧道两端都选择 “Disable”，不使用认证。

9. 选择密钥管理。选择 Auto(IKE)和在预享密钥栏输入一串数字或者字母。勾选框旁 PFS

图F－28：VPN标签

（Perfect Forward Secrecy 的缩写），以确保初始密钥交换和 IKE 方案是安全的您可以使用多达 24 个数字或者字母的任意组合，不允许特殊字符或者空格。在密钥生存期栏，您可以选择在一段时间后失效。输入您想密钥有效秒数，或者留空让密钥永久有效。

10． 点击“Save Settings”按钮。

您的隧道现在就建立了。

附录 G: SNMP 功能

SNMP(简单网络管理协议）是广泛使用的网络监视及管理协议。数据通过 SNMP 代理（例如本 VPN 路由器）到用作监视网络的工作站的控制台，然后路由器返回包含在管理信息库（MIB）里的信息。MIB 是一个数据结构，定义从网络设备能得到的信息，设备控制情况（被关闭和重启等）。

如果没有第三方管理软件，SNMP 功能如统计表，配置及设备信息将不可用。

本 VPN 路由器兼容所有 HP Openview 适应软件。

H: 术语表

Adapter（适配器）：一个增加计算机网络功能的设备。

Bit（位）： 二进制的位。

Boot ：设备启动。

Bridge：一种用来连接两种网络的设备。

Broadband（宽带）：一个永远在线，快速的互联网连接。

Browser（浏览器）：一个应用程序 提供了在万维网上浏览交换信息的方法。.

Buffer（缓冲器）：一个共享或指派的内存区，其用来支持协调不同计算和网络活动以避免相互阻塞。

Cable Modem：一个用来连接 PC 和有线电视网络，使其可以连上互联网的设备。

DDNS (动态域名系统)： 允许用一个固定域名称及动态 IP 作为站点，FTP 服务器或邮件服务器。

DHCP（动态主机配置协议）：一种协议，用来将限制一定时间租借的临时 IP 地址而非固定 IP 地址分配给局域网的计算机。

DMZ：一部分的 PC 不受防火墙保护，并且可以从互联网直接访问。

DNS (域名系统)： 互联网服务提供商的IP地址，其将站点的名字,翻译为IP地址。

Domain（域）：一个计算机群组成网络的特殊名称。

Download：在网络上接收文件传输。

DSL：一个通过电话线拥有在线宽带的设备。

Dynamic IP Address ： 一个由DHCP服务器指派的临时IP地址。

Encryption(加密) ： 对在网络传输的数据进行编码。

Ethernet（以太网） ： IEEE 标准网络协议定义数据如何放上普通传输介质及如何接收。

Finger（查找器） ： 查找与mail邮件地址关联的用户名的程序。

Firewall （防火墙）：-位于网络网关服务器的软件的组合，通常用来防止从外部网络到内部网络的未授权访问。

Firmware ： 运行网络设备的程序代码。

FTP (**文件传送[输]协议**）：在TCP/IP网络用于文件传送(输)的协议。

Gateway ：一种把二个具有不同网络协议的计算机网联接起来的操作装置。

Hardware（硬件）：硬件计算机及其它直接参与数据运算或信息交流的物理设备。

HTTP (HyperText Transport Protocol) ：WWW服务程序所用的协议。

IEEE (电子电气工程师协会) ：一个开发通信和网络标准的专业化组织。

IP (**网际协议**）： 用于在网络上传送数据的协议。

IP Address（IP地址）：地址用于标示网络或子网中独立的主机。

IPCONFIG ：Win2000及XP系统下用于显示详细网络设备IP地址的命令。

IPSec (网际协议安全)：虚拟个人网络协议用于实现在IP层安全地交换数据包。

ISP (互联网服务提供商)：一个提供访问互联网服务的公司。

LAN ：计算机和相关设备组成的网络。

MAC Address (介质访问控制地址) ：制造商分派到网络设备的唯一的地址。

Mbps (**兆比特每秒**）：兆比特每秒，传送数据的测量单位。

mIRC ：运行在Windows 下面，提供互联网转播聊天的程序。

Multicasting ：一次传送数据到一组目的地。

NAT (网络地址转换)： NAT技术转换本地网络地址到互联网上不同的IP地址。

Network（网(络)：一系列电脑或者装置用于彼此分享存储传送数据。

NNTP（网络新闻传输协议）：用来连接到互联网上的Usenet组的协议。

Node（节点）：一个网络的接入或者连接点，典型的是一台计算机或者工作站。

Packet（数据包）：通过网络发送的一个数据单元。

Ping（Packet InterNet Gopher）：一个用来判断一个特殊IP地址是否在线的互联网工具。

POP3 (邮局协议)：邮局协议,用于电子邮件的接收。

Port（端口）：在计算机或者网络设备用于插入电视电缆或者适配器的连接点。

PPPoE（Point-to-Point Over Ethernet）：一种特殊的广域网的传输协议，它提供认证，数据传输方式。

PPTP（Point-to-Point Tunnel Protocol）：一种虚拟私有网络的协议，它可以让PPP封包通过IP层。

这种协议也是用于欧洲地区的一种宽带连接类型。

Router（路由器）： 把多个网络连接起来的网络设备。

Server（服务器）：在一个网络中提供文件访问，打印，通信等功能的计算机。

SMTP (Simple Mail Transfer Protocol，简单邮件传输协议）： 标准的电子邮件传输协议。

SNMP (Simple Network Management Protocol，简单网络管理协议）： 广泛使用的网络控制管理协议。

Software（软件）：计算机的指令集。一系列指令用来执行一个特殊的任务称为一个“程序”。

Static IP Address（静态IP地址）： 指定到计算机或设备的固定地址。

Static Routing(静态路由)：在互联网通过一条固定路径转发数据。

Subnet Mask（子网掩码）：判定网络大小的一个地址码。

Switch（交换机）：也称交换式集线器，也用于连接多个网络节点，但与集线器不同，它的每端口独占固定带宽，各端口设备能并行传递数据而互不影响。

TCP（Transmission Control Protocol,传输控制协议）：TCP协议是为了在主机间实现高可靠性的包交换传输协议。

TCP/IP（Transmission Control Protocol/Internet Protocol,传输控制协议/网间协议）：是目前应用最为广泛的用于在网络中实现数据传输的协议，也是互联网所采用的网络协议，它根据网络中各节点独有的IP地址来选择路径，找到相应目的节点。

Telnet－一个用户命令的TCP/IP协议，用于访问远程主机。

TFTP（Trivial File Protocol，小文件传输协议）：是一个传输文件的简单协议，它基于UDP协议而实现。

Throughput （通过量）：从一个节点到另一个节点在给定时间成功传送的数据量。

UDP (用户数据报协议)：一个不需知道所传数据是否接收的数据传输网络协议 。

Upgrade（升级）：用新版本软件或固件来替换旧版。

URL (Uniform Resource Locator) ：文件位于互联网的地址

VPN (Virtual Private Network，虚拟个人网络)：用来保护通过互联网从一个网络到另一个网络的数据的安全措施。

WAN (Wide Area Network，广域网)：互联网。

WINIPCFG ： Windows 98及Me系统下用于显示详细网络设备IP地址的命令。

附录 I：规格

型号：BEFSX41-CN

标准：IEEE 802.3 (10BaseT), IEEE 802.3u (100BaseTX)

端口：一个10Base-T RJ-45互联网端口
四个10/100 RJ-45以太网端口
一个电源端口

按钮：复位Reset按钮

缆线类型：非屏蔽5类线以上

指示灯：电源，DMZ，以太网（1-4），互联网

尺寸：186 mm x 48 mm x 154mm（7.32" x 1.88" x 6.06"）

重量：0.38 kg（13.40 oz）

电源：外接，12V DC，1000mA

认证：FCC Class B，CE标志，VCCI

工作温度：0ºC to 40ºC (32ºF to 104ºF)

储存温度：-20ºC to 70ºC (-4ºF to 158ºF)

工作湿度：0% to 85%，非冷凝

储存湿度：5% to 90%，非冷凝

附录 J：保修信息

请确认取得您的购买证明，当您需要协助时并提供来自产品上的序列号(S/N)，当无购买证明，将无法对您的产品进行保修服务。

附录 K:联系信息

请使用下列电话或互联网地址联系 LINKSYS 技术支持。

技术支持

电话：800-810-5704

电子邮件支持

chinasupport@linksys.com

网站:

http://www.linksys.com/cn

销售咨询

chinasales@linksys.com